Vera C. Rubin Observatory
Rubin Observatory Operations

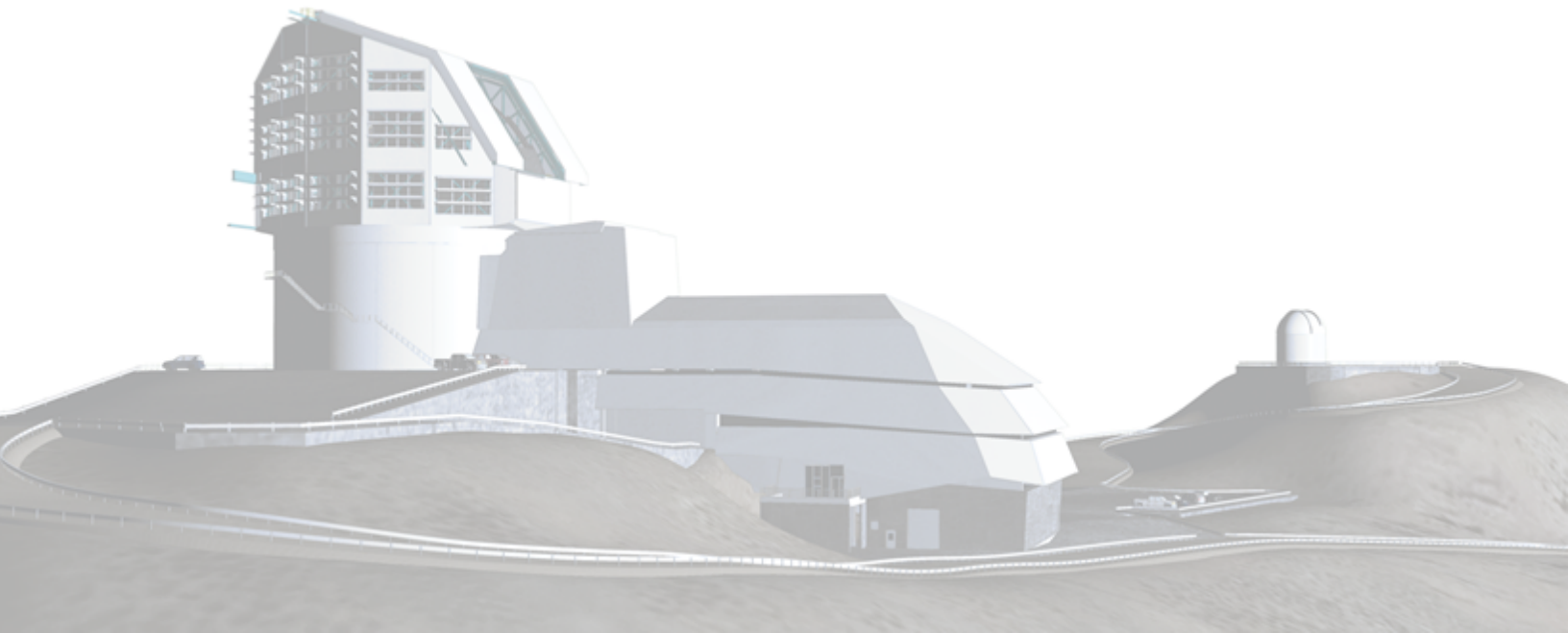
Pixel Zone system security plan

William O'Mullane

RTN-082

Latest Revision: 2025-04-10

DRAFT



Abstract

This document provides the mapping to NIST800-171 for the Rubin Pixel Zone.

Change Record

Version	Date	Description	Owner name
0.1	2024-07-05	Initial Draft	William O'Mullane
0.2	2024-07-15	Variance, Waiver Language	William O'Mullane
0.3	2025-04-10	Update afterr pixel zone firewall in place	William O'Mullane

Document source location: `https://github.com/lsst/rtn-082`

Contents

Pixel Zone system security plan

1 Introduction and Scope

Vera C. Rubin Observatory will observe the night sky with unprecedented frequency and depth. Per DMTN-199, NIST.SP.800-171r3 is applicable to our pixel data. This document provide the security plan for the *Pixel Zone* which encompasses the areas where data is held in NSF facilities. The SLAC facilities are covered in *NEED REF*.

In accordance with NIST.FIPS.200 and DMTN-199 the security category is :

$$SC_{Pixel\,Zone} = \{(\textbf{confidentiality}, \text{moderate}), (\textbf{integrity}, \text{low}), (\textbf{availability}, \text{low})\} \quad (1)$$

The technology implementation details may be found in ITTN-074.

This plan should be reviewed at least annually.

2 Minimum security requirements

NIST.FIPS.200 declares 17 security related areas that should be covered, each is given a sub section here. A detailed compliance with NIST.SP.800-171r3 is given in Appendix A. Here we also mention the controls, as outlined in the CUI overlay of NIST.SP.800-171r3, we aim to implement in each section.

2.1 Access Control (AC)

Access to the *Pixel Zone* is restricted to approved account holders. See ITTN-010 and ITTN-045 (AC-01 Policy and Procedures).

Account creation is tracked with Jira tickets and requires manager approval (AC-02 Account Management).

Unix groups are used to restrict individual user access and effectively provide *account types*

(AC-03 Access Enforcement). Sudo is used for escalation by users who are allowed privileged access - use is logged.

DMTN-199 defines the control flow for pixel data (AC-04 Information Flow Enforcement).

Accounts are locked out after 6 failed attempts to log in (AC-07 Unsuccessful Logon Attempts).

Message of the day shall declare the Pixel zone security (Use Notification AC-08).

Sessions are terminated every 24 hours (AC-12 Session Termination).

Remote access is granted via an group membership. 2FA VPN is required for any remote access (remote access AC-17).

Access to summit WiFi is controlled via registered MAC address. Even on the summit WiFi VPN login is required to access the *Pixel Zone* (wireless access AC-18).

We do not allow pixel data to be copied to external devices (External System AC-20).

We have no public access (AC-22 Publicly Accessible Content)

We do not use specific *-admin* accounts - our team is small and we find such accounts less secure.

We shall review group membership for summit access at least once per year.

2.2 Awareness and Training (AT)

The access control plan (Marshall, ACP) indicates training etc. RTN-073 provides guidelines for embargo data access. Specific guidelines on communication channels have been shared with users in DMTN-286. (AT-01 Policy and Procedures)

Embargo training is mandatory for all users with access to pixel data within the embargo period. (AT-02 Literacy Training and Awareness) Training will be renewed annually.

2.3 Audit and Accountability (AU)

An *Observability system* has been built, on contract ITTN-070, to make this information useful to find incursions and anomalies(AU-02 Event Logging, AU-03 Content of Audit Records, AU-07 Audit Record Reduction and Report Generation, AU-12 Audit Record Generation).

Logs shall also be sent to the Research SOC for review (AU-06 Audit Record Review, Analysis, and Reporting).

Audit records have UTC timestamps (AU-08 Time Stamps).

We shall have sufficient log storage, currently 70TB, for 2 years of logs (AU-04 Audit Log Storage Capacity).

Logs shall be kept for at least 2 years (AU-11 Audit Record Retention).

Squadcast is used for alerting on system failures (AU-05 Response to Audit Logging Process Failures).

Logs and audit information are secured for access only by the Chile DevOps team(AU-09 Protection of Audit Information).

2.4 Certification, Accreditation, and Security Assessments (CA)

We are a small team however we regularly assess our security posture and adjust where needed (CA-02 Control Assessments). We shall carry out PEN testing nominally annually but at least every other year. Training was organised for the Chile DevOps team and some individuals will pursue accreditation/certification.

2.5 Configuration Management (CM)

Higher level or broader changes go to an operations CCB RTN-072 (CM-01 Policy and Procedures). Otherwise we run almost exclusively infrastructure as code - our baseline is in github. Changes follow the DM change process - reviews and tests required for any change (CM-03 Configuration Change Control).

The applications deployed and their configurations are all dealt with via our phalanx[1] system (CM-02 Baseline Configuration, CM-08 System Component Inventory).

Pixel data is only located in the pixel zone and embargo rack (CM-12 Information Location).

We do not have a definitions of high-risk areas and therefore we do not apply specific configurations to devices during travel.

2.6 Contingency Planning (CP)

Disaster recovery and incident reporting is covered in RTN-030 (CP-01 Policy and Procedures)

2.7 Identification and Authentication (IA)

IA is covered in ITTN-010 (IA-01 Policy and Procedures). Users are associated with their unique accounts (IA-02 Identification and Authentication). Re-authentication is once per 24 hours (IA-11 Re-Authentication).

Access to the *Pixel Zone* is via 2FA VPN. Devices connection to our networks are know by MAC address.

Typically 1password generated passwords are used and any sharing is done using vaults (IA-05 Authenticator Management). Passwords must by at least 8 chars, use 2 character classes and can not be reused for 10 goes.

All new users are known to admins or confirmed by a manager (IA-12 Identity Proofing).

2.8 Incident Response (IR)

Incident response is covered in RTN-030 §3 (IR-01 Policy and Procedures).

[1] `https://phalanx.lsst.io`

2.9 Maintenance (MA)

We have weekly maintenance windows for summit systems, one each for Infrastructure, Applications, and Control System (MA-01 Policy and Procedures)

Activities are tickets and discussed in stand up meetings (MA-02 Controlled Maintenance).

All tools go through the usual procurement process and maintenance equipment does not and will not hold pixel data (MA-03 Maintenance Tools).

Maintenance is carried out by our personnel (MA-05 Maintenance Personnel).

2.10 Media Protection (MP)

Pixel Zone is all about protecting data in the embargo period as per DMTN-199 (MP-01 Policy and Procedures).

Access is controlled via IPA groups and 2Fa VPN (MP-02 Media Access). Data will never be on removable media. We do not allow media to be mounted to machines int he pixel zone.

Pixel data exists on disk in only three locations during the embargo period, there are no further backups of this so no copy on removable media.

2.11 Physical and Environmental Protection (PE)

Computer rooms have key card access and are restricted to a limited number of personnel (PE-02 Physical Access Authorizations, PE-03 Physical Access Control). Racks have further locks and door sensors installed. There are cameras with motion detection functions installed in the computer rooms.

The DWDM (transmission devices) are within the controlled computer room in a locked rack (PE-04 Access Control for Transmission).

Access is logged and logs are kept for up to three years, all the equipment being installed is HID and complies with section 889 of the John S. McCain National Defense Authorization Act

(NDAA) (PE-06 Monitoring Physical Access).

Remote work is allowed from anywhere with access via 2FA VPN (PE-17 Alternate Work Site).

2.12 Planning (PL)

RTN-030 provides pointers to the many information security related documents (PL-01 Policy and Procedures).

Rubin has an acceptable use policy augmented by RTN-073 and DMTN-286 for embargoed data (PL-04 Rules of Behavior).

2.13 Personnel Security (PS)

Only team members will have access to embargo images. All staff are known individuals screened on hiring (PS-01 Policy and Procedures, PS-03 Personnel Screening). In kind contributors working with data are known scientists and all go though FACTs checks to get accounts at USDF.

Where appropriate on termination all account access is removed - some off-boards remain collaborators (PS-04 Personnel Termination).

2.14 Risk Assessment (RA)

This is part of our regular risk assessment process RDO-71 but we also look in depth at specific applications(RA-01 Policy and Procedures).

Mostly we have concentrated the application exposure in phalanx which is carefully assessed and monitored. However we do perform specific security risk assessment where it is considered most needed e.g. SQR-041 for the science platform which is one of our major attack surfaces (RA-03 Risk Assessment).

We have conducted external PEN testing and shall do so annually in addition to using available scanning tools (RA-05 Vulnerability Monitoring and Scanning).

2.15 System and Services Acquisition (SA)

Security for our external facing applications have been encapsulated in Phalanx. (SA-01 Policy and Procedures) This allows a single team to take care of AAA for all applications to minimize the attack surface. The number of applications which can touch the embargoed data is also small and they are behind the 2Fa VPN.

We apply several principles: (SA-08 Security and Privacy Engineering Principles):

- Least Privilege : we try to reduce the number of accounts with privileges
- Minimize attack surface: phalanx really helps with this but also using 2FA and VPN for pixel zone.
- Access control mechanisms: we use tokens for inter application access
- Defense in depth: we are attempting to know when we have been hit
- Open design: our security does not rely on secrecy of design our designs are public
- Economy of mechanism: we always attempt the simplest solution

Our policy is to replace components before they reach EOL (SA-22 Unsupported System Components).

2.16 System and Communications Protection (SC)

DMTN-286 and SITCOMTN-076 cover communication for embargoed data (SC-01 Policy and Procedures).

Embargo data are kept on encrypted disks using OS level encryption (SC-04 Information in Shared System Resources). 2FA VPN is required to access the *Pixel Zone* . We isolate internal traffic on different VLANs. Bastion hosts are used for access to deeper internal systems.

Border firewalls prevent some repeated attacks, confirmed by PEN testing (SC-05 Denial-of-service Protection, SC-07 Boundary Protection).

Data transmission to SLAC is via secure routers with AES-256 encryption (SC-08 Transmission Confidentiality and Integrity).

Connections are rest each 24 hour period (SC-10 Network Disconnect).

Encryption keys are managed by specific key services (SC-12 Cryptographic Key Establishment and Management).

Embargo data are kept on encrypted disks using OS level encryption at rest (SC-28 Protection of Information at Rest).

2.17 System and Information Integrity (SI)

RTN-030 details specific policies (SI-01 Policy and Procedures).

We respond immediately to any security issue. It receives top priority. Reported vulnerabilities are dealt with within 24 hours (SI-02 Flaw Remediation).

A Compliance with NIST800.171

Please note the following definitions:

- Waiver - not applicable to the operation
- Variance - cannot be implemented due to operational constraints but have a compensating control applied
- Exception - cannot be implemented due to operational constraints (no compensating control applied)

Table 1: This table provides an overview of the NIST.SP.800-171r3 and Rubin compliance with it.

NIST 800-171r3	2024 Status	Intended Compliance	Note
3.1 ACCESS CONTROL			

03.01.01 Account Management a. Define the types of system accounts allowed and prohibited. b. Create, enable, modify, disable, and remove system accounts in accordance with policy, procedures, prerequisites, and criteria. c. Specify: 1. Authorized users of the system, 2. Group and role membership, and 3. Access authorizations (i.e., privileges) for each account. d. Authorize access to the system based on: 1. A valid access authorization and 2. Intended system usage. e. Monitor the use of system accounts. f. Disable system accounts when: 1. The accounts have expired, 2. The accounts have been inactive for [Assignment: organization-defined time period], 3. The accounts are no longer associated with a user or individual, 4. The accounts are in violation of organizational policy, or 5. Significant risks associated with individuals are discovered. g. Notify account managers and designated personnel or roles within: 1. [Assignment: organization-defined time period] when accounts are no longer required. 2. [Assignment: organization-defined time period] when users are terminated or transferred. 3. [Assignment: organization-defined time period] when system usage or the need-to-know changes for an individual. h. Require that users log out of the system after [Assignment: organization-defined time period] of expected inactivity or when [Assignment: organization-defined circumstances].	Y	Y	IPA groups are in place for summit which restrict privileges of individual users. Off boarding and account disabling in place - considering active account with monthly reaffirmation instead. See https://ittn-010.lsst.io/
03.01.02 Access Enforcement Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.	Y	Y	IPA groups are in place on the summit restricting users abilities. Legacy systems use the active directory groups for this.
03.01.03 Information Flow Enforcement Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.	Y	Y	DMTN-199 defines the control flow for pixel data. Its implementation enforces it.
03.01.04 Separation of Duties a. Identify the duties of individuals requiring separation. b. Define system access authorizations to support separation of duties.	V	Y	Principle of least privilege is applied. Some users have access to hosts that is unneeded.
03.01.05 Least Privilege a. Allow only authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks. b. Authorize access to [Assignment: organization-defined security functions] and [Assignment: organization-defined security-relevant information]. c. Review the privileges assigned to roles or classes of users [Assignment: organization-defined frequency] to validate the need for such privileges. d. Reassign or remove privileges, as necessary.	V	Y	IPA groups are in place for summit which restrict privileges of individual users. Off boarding and account disabling in place - considering active account with monthly reaffirmation instead. See https://ittn-010.lsst.io/
03.01.06 Least Privilege – Privileged Accounts a. Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles]. b. Require that users (or roles) with privileged accounts use non-privileged accounts when accessing non-security functions or non-security information.	V	W	These accounts were specifically target in the Gemini attack - we would rather not use this approach.
03.01.07 Least Privilege – Privileged Functions a. Prevent non-privileged users from executing privileged functions. b. Log the execution of privileged functions.	Y	Y	a. sudo must be used for privileged functions b. We log sudo attempts .
03.01.08 Unsuccessful Logon Attempts a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]. b. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action] when the maximum number of unsuccessful attempts is exceeded.	Y	Y	Web Services such as love, foreman, IPA console, nublado, etc. may need rate limiting. We don't use passwords in ssh hosts, only ssh keys (which many consider more secure). We are not aware of a retry limit for ssh-key access; an appropriate extra level of security would be to not use the default port 22. However, we do limit attempts to 6 with a block of 600 minutes, which will effectively block failed SUDO logins.
03.01.09 System Use Notification. Display a system use notification message with privacy and security notices consistent with applicable CUI rules before granting access to the system.	N	Y	Check login notices etc. A login banner can be displayed upon login

03.01.10 Device Lock a. Prevent access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended]. b. Retain the device lock until the user reestablishes access using established identification and authentication procedures. c. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	Y	Y	This is our policy.
03.01.11 Session Termination. Terminate a user session automatically after [Assignment: organization-defined conditions or trigger events requiring session disconnect].	Y	Y	ssh sessions are generally not limited on hosts but VPN will timeout daily; some network equipment has timeouts set;
03.01.12 Remote Access a. Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access. b. Authorize each type of remote system access prior to establishing such connections. c. Route remote access to the system through authorized and managed access control points. d. Authorize the remote execution of privileged commands and remote access to security-relevant information.	Y	Y	We currently check who and from where is connecting. IPA groups control access (and 2FA VPN). Bastion nodes are used to control ingress. UNIX groups are used at SLAC for access control.
03.01.13 Withdrawn	W		Withdrawn in revision 3
03.01.14 Withdrawn	W		Withdrawn in revision 3
03.01.15 Withdrawn	W		Withdrawn in revision 3
03.01.16 Wireless Access a. Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system. b. Authorize each type of wireless access to the system prior to establishing such connections. c. Disable, when not intended for use, wireless networking capabilities prior to issuance and deployment. d. Protect wireless access to the system using authentication and encryption.	Y	Y	All devices attaching in Chile need to be registered by Mac address. We further consider still requiring 2FA VPN to access privileged systems from the WiFi.
03.01.17 Withdrawn	W		Withdrawn in revision 3
03.01.18 Access Control for Mobile Devices a. Establish usage restrictions, configuration requirements, and connection requirements for mobile devices. b. Authorize the connection of mobile devices to the system. c. Implement full-device or container-based encryption to protect the confidentiality of CUI on mobile devices.	Y	Y	Mobile devices must be registered on the summit - mobile devices do not contain pixel data. In the case where an image may exist on say commissioning team laptop we will have disk encryption enabled.
03.01.19 Withdrawn	Y	Y	Withdrawn in revision 3
03.01.20 Use of External Systems a. Prohibit the use of external systems unless the systems are specifically authorized. b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements]. c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after: 1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and 2. Retaining approved system connection or processing agreements with the organizational entities hosting the external systems. d. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.	N	Y	We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices on the pixel zone.
03.01.21 Withdrawn	W		Withdrawn in revision 3
03.01.22 Publicly Accessible Content a. Train authorized individuals to ensure that publicly accessible information does not contain CUI. b. Review the content on publicly accessible systems for CUI and remove such information, if discovered.	Y	Y	We do not intend to post images on publicly accessible systems. (DMTN-286). We intend to roll out training.
3.2 AWARENESS AND TRAINING			

03.02.01 Literacy Training and Awareness a. Provide security literacy training to system users: 1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter, 2. When required by system changes or following [Assignment: organization-defined events], and 3. On recognizing and reporting indicators of insider threat, social engineering, and social mining. b. Update security literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Y	Y	A specific course for DMTN-199 is in prep. Each org has cyber security training already.
03.02.02 Role-Based Training a. Provide role-based security training to organizational personnel: 1. Before authorizing access to the system or CUI, before performing assigned duties, and [Assignment: organization-defined frequency] thereafter 2. When required by system changes or following [Assignment: organization- defined events]. b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	V	Y	OUO training at SLAC, DMTN-199 training for commissioners, Specific training for satellite catalog handlers. We would like to do more here like capture flag exercises for developers or blue/red teams events. Cyber training is annual.
03.02.03 Withdrawn	W		Withdrawn in revision 3
3.3 AUDIT AND ACCOUNTABILITY			
03.03.01 Event Logging a. Specify the following event types selected for logging within the system: [Assignment: organization-defined event types]. b. Review and update the event types selected for logging [Assignment: organization-defined frequency].	Y	Y	Observability contract.
03.03.02 Audit Record Content a. Include the following content in audit records: 1. What type of event occurred 2. When the event occurred 3. Where the event occurred 4. Source of the event 5. Outcome of the event 6. Identity of the individuals, subjects, objects, or entities associated with the event b. Provide additional information for audit records as needed.	Y	Y	
03.03.03 Audit Record Generation a. Generate audit records for the selected event types and audit record content specified in 03.03.01 and 03.03.02. b. Retain audit records for a time period consistent with the records retention policy.	Y	Y	Observability system
03.03.04 Response to Audit Logging Process Failures a. Alert organizational personnel or roles within [Assignment: organization-defined time period] in the event of an audit logging process failure. b. Take the following additional actions: [Assignment: organization-defined additional actions].	N	Y	
03.03.05 Audit Record Review, Analysis, and Reporting a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications and the potential impact of inappropriate or unusual activity. b. Report findings to organizational personnel or roles. c. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	N	Y	Again shall look for third party contract for this
03.03.06 Audit Record Reduction and Report Generation a. Implement an audit record reduction and report generation capability that supports audit record review, analysis, reporting requirements, and after-the-fact investigations of incidents. b. Preserve the original content and time ordering of audit records.	Y	Y	Observability system
03.03.07 Time Stamps a. Use internal system clocks to generate time stamps for audit records. b. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or include the local time offset as part of the time stamp.	Y	Y	
03.03.08 Protection of Audit Information a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion. b. Authorize access to management of audit logging functionality to only a subset of privileged users or roles.	Y	Y	Only specific admin users have access to audit logs
03.03.09 Withdrawn	W		Withdrawn in revision 3
3.4 CONFIGURATION MANAGEMENT			

03.04.01 Baseline Configuration a. Develop and maintain under configuration control, a current baseline configuration of the system. b. Review and update the baseline configuration of the system [Assignment: organization-defined frequency] and when system components are installed or modified.	Y	Y	We use mainly infrastructure as code approaches so the software is well tracked. IT inventory all the hardware.
03.04.02 Configuration Settings a. Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings]. b. Identify, document, and approve any deviations from established configuration settings.	Y	Y	Configuration settings are defined and documented in the lsst-it rancher, puppet and phalanx repos.
03.04.03 Configuration Change Control a. Define the types of changes to the system that are configuration-controlled. b. Review proposed configuration-controlled changes to the system, and approve or disapprove such changes with explicit consideration for security impacts. c. Implement and document approved configuration-controlled changes to the system. d. Monitor and review activities associated with configuration-controlled changes to the system.	Y	Y	We have an operations CCB (https://rtn-072.lsst.io/) and code change process in place which also cover the infrastructure as code.
03.04.04 Impact Analyses a. Analyze changes to the system to determine potential security impacts prior to change implementation. b. Verify that the security requirements for the system continue to be satisfied after the system changes have been implemented.	Y	Y	Continuous integrations checks on puppet and phalanx check any changes prior to test deploy which is done prior to production.
03.04.05 Access Restrictions for Change Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	Y	Y	At infrastructure level this is is controlled by the Chile DevOps team.
03.04.06 Least Functionality a. Configure the system to provide only mission-essential capabilities. b. Prohibit or restrict use of the following functions, ports, protocols, connections, and services: [Assignment: organization-defined functions, ports, protocols, connections, and services]. c. Review the system [Assignment: organization-defined frequency] to identify unnecessary or nonsecure functions, ports, protocols, connections, and services. d. Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.	Y	Y	Most application level functionality is controlled via phalanx. The OS level is puppet controlled.
03.04.07 Withdrawn	W		Withdrawn in revision 3
03.04.08 Authorized Software – Allow by Exception a. Identify software programs authorized to execute on the system. b. Implement a deny-all, allow-by-exception policy for the execution of authorized software programs on the system. c. Review and update the list of authorized software programs [Assignment: organization-defined frequency].	Y	Y	SUDO lists restrict access so users can not install applications on the summit nor in SLAC (outside a container). Mainly we containerize the applications and have users work within deployed containers. All containers are controlled/deployed via phalanx configuration.
03.04.09 Withdrawn	W		Withdrawn in revision 3
03.04.10 System Component Inventory a. Develop and document an inventory of system components. b. Review and update the system component inventory [Assignment: organization-defined frequency]. c. Update the system component inventory as part of installations, removals, and system updates.	Y	Y	phalanx.lsst.io
03.04.11 Information Location a. Identify and document the location of CUI and the system components on which the information is processed and stored. b. Document changes to the system or system component location where CUI is processed and stored.	Y	Y	DMTN-199- Embargo rack and pixel zones are our places for restricted items.
03.04.12 System and Component Configuration for High-Risk Areas a. Issue systems or system components with the following configurations to individuals traveling to high-risk locations: [Assignment: organization-defined system configurations]. b. Apply the following security requirements to the systems or components when the individuals return from travel: [Assignment: organization-defined security requirements].	N	Y	Though people self select to remove vaults and carry clean personal devices we do not have a strict policy nor do we have a list of high risk areas. In general there is no data on peoples machines so it is account/password vulnerability we would need to cover.
3.5 IDENTIFICATION AND AUTHENTICATION			

03.05.01 User Identification and Authentication a. Uniquely identify and authenticate system users, and associate that unique identification with processes acting on behalf of those users. b. Re-authenticate users when [Assignment: organization-defined circumstances or situations requiring re-authentication].	Y	Y	Users are associated with their unique Unix accounts. Re-authentication is once per 24 hours.
03.05.02 Device Identification and Authentication Uniquely identify and authenticate [Assignment: organization-defined devices or types of devices] before establishing a system connection.	Y	Y	Users access via VPN with a 2FA device (DUO or 1password)
03.05.03 Multi-Factor Authentication Implement multi-factor authentication for access to privileged and non-privileged accounts.	Y	Y	Summit uses 2FA - SLAC do no require this.
03.05.04 Replay-Resistant Authentication Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.	Y	Y	Lockout after six failures.
03.05.05 Identifier Management a. Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier. b. Select and assign an identifier that identifies an individual, group, role, service, or device. c. Prevent the reuse of identifiers for [Assignment: organization-defined time period]. d. Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	Y	Y	a. Jira tickets are used and management approval requested b. Unique id is chosen c. last 10 passwords can not be used d. Single sign on across all systems uses same id. See also https://ittn-045.lsst.io/
03.05.06 Withdrawn	W		Withdrawn in revision 3
03.05.07 Password Management a. Maintain a list of commonly-used, expected, or compromised passwords, and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised. b. Verify that passwords are not found on the list of commonly used, expected, or compromised passwords when users create or update passwords. c. Transmit passwords only over cryptographically protected channels. d. Store passwords in a cryptographically protected form. e. Select a new password upon first use after account recovery. f. Enforce the following composition and complexity rules for passwords: [Assignment: organization-defined composition and complexity rules].	Y	Y	a. For the few system passwords we have a generator is used such as 1password. b. We do use https://haveibeenpwned.com/Passwords c. Passwords than must be shared are shared via 1password vaults. For users onetimesecret is used to pass an initial password which must then be replaced. d. 1password is used for passwords e. account recovery typically starts with a new password the user must then replace. f. complex passwords are required.
03.05.08 Withdrawn	W		Withdrawn in revision 3
03.05.09 Withdrawn	W		Withdrawn in revision 3
03.05.10 Withdrawn	W		Withdrawn in revision 3
03.05.11 Authentication Feedback Obscure feedback of authentication information during the authentication process.	Y	Y	Passwords are not echoed on any system.
03.05.12 Authenticator Management a. Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution. b. Establish initial authenticator content for any authenticators issued by the organization. c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators. d. Change default authenticators at first use. e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events]. f. Protect authenticator content from unauthorized disclosure and modification.	Y	Y	This applies mainly to passwords for us. We pass passwords with onetimesecret and then ask the user to change it immediately.
3.6 INCIDENT RESPONSE			
03.06.01 Incident Handling Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.	Y	Y	Incident handling/response is in place. AURA also have insurance for serious incursions.
03.06.02 Incident Monitoring, Reporting, and Response Assistance a. Track and document system security incidents. b. Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]. c. Report incident information to [Assignment: organization-defined authorities]. d. Provide an incident response support resource that offers advice and assistance to system users on handling and reporting incidents.	Y	Y	We track and report incidents. AURA insurance can provide further support if needed.
03.06.03 Incident Response Testing Test the effectiveness of the incident response capability [Assignment: organization-defined frequency].	Y	Y	This was done at least with the PEN testing - which we shall repeat.

03.06.04 Incident Response Training a. Provide incident response training to system users consistent with assigned roles and responsibilities: 1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access, 2. When required by system changes, and 3. [Assignment: organization-defined frequency] thereafter. b. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Y	Y	Cyber training includes user level incident response i.e. who to report attempts to.
03.06.05 Incident Response Plan a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability, 2. Describes the structure and organization of the incident response capability, 3. Provides a high-level approach for how the incident response capability fits into the overall organization, 4. Defines reportable incidents, 5. Addresses the sharing of incident information, and 6. Designates responsibilities to organizational entities, personnel, or roles. b. Distribute copies of the incident response plan to designated incident response personnel (identified by name and/or by role) and organizational elements. c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing. d. Protect the incident response plan from unauthorized disclosure.	Y	Y	RTN-030 Section 3.
3.7 MAINTENANCE			
03.07.01 Withdrawn	W		Withdrawn in revision 3
03.07.02 Withdrawn	W		Withdrawn in revision 3
03.07.03 Withdrawn	W		Withdrawn in revision 3
03.07.04 Maintenance Tools a. Approve, control, and monitor the use of system maintenance tools. b. Check media with diagnostic and test programs for malicious code before it is used in the system. c. Prevent the removal of system maintenance equipment containing CUI by verifying that there is no CUI on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility.	Y	Y	a. Maintenance tools go through the requisition process - hence at least 2 managers approve. b. We run scans on downloaded media. c. Maintenance equipment does not have CUI on it.
03.07.05 Nonlocal Maintenance a. Approve and monitor nonlocal maintenance and diagnostic activities. b. Implement multi-factor authentication and replay resistance in the establishment of nonlocal maintenance and diagnostic sessions. c. Terminate session and network connections when nonlocal maintenance is completed.	Y	Y	a. Activities are always Jira ticketed b. 2FA is always needed to access pixel zone. c. Policy is to log off when done.
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations.	Y	Y	In general our staff do the maintenance. On occasion when we have remote assistance credentials are granted for a limited time and work is carried out with our staff.
3.8 MEDIA PROTECTION			
03.08.01 Media Storage Physically control and securely store system media that contain CUI.	Y	Y	Pixel Zone and Embargo Rack
03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles.	Y	Y	Pixel Zone and Embargo Rack
03.08.03 Media Sanitization Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse.	Y	Y	We format/clean all devices prior to disposal/reuse.
03.08.04 Media Marking Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings.	Y	Y	We do not use any removable media for embargo information.
03.08.05 Media Transport a. Protect and control system media that contain CUI during transport outside of controlled areas. b. Maintain accountability of system media that contain CUI during transport outside of controlled areas. c. Document activities associated with the transport of system media that contain CUI.	Y	Y	We do not use any removable media for embargo information. All transfers are over secure links.
03.08.06 Withdrawn	W		Withdrawn in revision 3

03.08.07 Media Use a. Restrict or prohibit the use of [Assignment: organization-defined types of system media]. b. Prohibit the use of removable system media without an identifiable owner.	N	Y	Can be rolled out with puppet but there are some servers require USB to be enabled but are in the server room. We can disable USB disk mounts at OS level. The machines and filesystem are encrypted so even if someone rebooted a node from a device to allow mounting USB they still could not get any data.
03.08.08 Withdrawn	W		Withdrawn in revision 3
03.08.09 System Backup – Cryptographic Protection a. Protect the confidentiality of backup information. b. Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI at backup storage locations.	Y	Y	Pixel data is in only three locations - two in Chile and SLAC. There are no backups during embargo.
3.9 PERSONNEL SECURITY			
03.09.01 Personnel Screening a. Screen individuals prior to authorizing access to the system. b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening].	Y	Y	Only project team members will have access to early images - all are known individuals screened on hiring. This doesn't suggest background security screening and it was also explicitly not required by the agencies in section 2 of the requirements document.
03.09.02 Personnel Termination and Transfer a. When individual employment is terminated: 1. Disable system access within [Assignment: organization-defined time period], 2. Terminate or revoke authenticators and credentials associated with the individual, and 3. Retrieve security-related system property. b. When individuals are reassigned or transferred to other positions in the organization: 1. Review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility, and 2. Modify access authorization to correspond with any changes in operational need.	Y	Y	This is the off boarding policy. Note that many collaborators retain some level of access even when off boarded.
3.10 PHYSICAL PROTECTION			
03.10.01 Physical Access Authorizations a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides. b. Issue authorization credentials for facility access. c. Review the facility access list [Assignment: organization-defined frequency]. d. Remove individuals from the facility access list when access is no longer required.	Y	Y	This physical access includes locks on server cabinets and key card access in base. (Contracted for summit computer room)
03.10.02 Monitoring Physical Access a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents. b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events].	Y	Y	Security is in place on Cerro Pachon and at the entrance to the mountain - though not only for Rubin so not permanently at the observatory.
03.10.03 Withdrawn	W		Withdrawn in revision 3
03.10.04 Withdrawn	W		Withdrawn in revision 3
03.10.05 Withdrawn	W		Withdrawn in revision 3
03.10.06 Alternate Work Site a. Determine alternate work sites allowed for use by employees. b. Employ the following security requirements at alternate work sites: [Assignment: organization-defined security requirements].	Y	Y	All work can be done remotely from any location via the 2FA VPN. Cyber training assumes remote work is common.
03.10.07 Physical Access Control a. Enforce physical access authorizations at entry and exit points to the facility where the system resides by: 1. Verifying individual physical access authorizations before granting access to the facility and 2. Controlling ingress and egress with physical access control systems, devices, or guards. b. Maintain physical access audit logs for entry or exit points. c. Escort visitors, and control visitor activity. d. Secure keys, combinations, and other physical access devices. e. Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.	Y	Y	a. Computer centers are restricted with key cards to appropriate staff - contractors are considered like staff. b. NOIRLab can currently store 80 gigs of data for audit logs of physical access, which will last at least three years - all the equipment being installed is HID and complies with section 889 of the John S. McCain National Defense Authorization Act (NDAA) c. visitors are escorted where appropriate i.e. where we have secure hardware. d. Individuals have cards/keys they are not left in insecure locations. e. we will not be printing images.
03.10.08 Access Control for Transmission Control physical access to system distribution and transmission lines within organizational facilities.	Y	Y	DWDM, secure routers are in card controlled room (summit contract pending)
3.11 RISK ASSESSMENT			
03.11.01 Risk Assessment a. Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI. b. Update risk assessments [Assignment: organization-defined frequency].	Y	Y	This is part of our regular risk assessment process but we also look in depth at specific applications. Mostly we have concentrated the application exposure in phalanx which is carefully assessed and monitored.

03.11.02 Vulnerability Monitoring and Scanning a. Monitor and scan the system for vulnerabilities [Assignment: organization- defined frequency] and when new vulnerabilities affecting the system are identified. b. Remediate system vulnerabilities within [Assignment: organization-defined response times]. c. Update system vulnerabilities to be scanned [Assignment: organization-defined frequency] and when new vulnerabilities are identified and reported.	Y	Y	a. We monitor constantly also conduct third party contract PEN testing b. We patch for vulnerabilities within 24 hours. c. third part applications are used for scanning
03.11.03 Withdrawn	W		
03.11.04 Risk Response Respond to findings from security assessments, monitoring, and audits.	Y	Y	We respond immediately to any security issue. It receives top priority.
3.12 SECURITY ASSESSMENT			
03.12.01 Security Assessment Assess the security requirements for the system and its environment of operation [Assignment: organization-defined frequency] to determine if the requirements have been satisfied.	Y	Y	Annual reviews
03.12.02 Plan of Action and Milestones a. Develop a plan of action and milestones for the system: 1. To document the planned remediation actions to correct weaknesses or deficiencies noted during security assessments and 2. To reduce or eliminate known system vulnerabilities. b. Update the existing plan of action and milestones based on the findings from: 1. Security assessments, 2. Audits or reviews, and 3. Continuous monitoring activities.	Y	Y	We use Jira ticketing for all work including security patches and improvements.
03.12.03 Continuous Monitoring Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.	Y	Y	Rubin is a mature organization with regular review and monitoring of all activities including cyber.
03.12.04 Withdrawn	W		Withdrawn in revision 3
03.12.05 Information Exchange a. Approve and manage the exchange of CUI between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements; other types of agreements]. b. Document interface characteristics, security requirements, and responsibilities for each system as part of the exchange agreements. c. Review and update the exchange agreements [Assignment: organization-defined frequency].	Y	Y	This is entirely governed by DMTN-199 and its change control process.
3.13 SYSTEM AND COMMUNICATIONS PROTECTION			
03.13.01 Boundary Protection a. Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system. b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. c. Connect to external systems only through managed interfaces that consist of boundary protection devices arranged in accordance with an organizational security architecture.	Y	Y	a. We have border scanning devices. b. We use VLANs and multiple VPNs to segment the network. c. Bastions are used where needed and 2FA VPN for all users to connect to pixel zone.
03.13.02 Withdrawn	W		Withdrawn in revision 3
03.13.03 Withdrawn	W		Withdrawn in revision 3
03.13.04 Information in Shared System Resources Prevent unauthorized and unintended information transfer via shared system resources.	Y	Y	DMTN-286 and SITCOMTN-076 cover ground rules on this
03.13.05 Withdrawn	W		
03.13.06 Network Communications – Deny by Default – Allow by Exception Deny network communications traffic by default, and allow network communications traffic by exception.	Y	Y	Routing and whitelisting is quite explicit.
03.13.07 Withdrawn			Withdrawn in revision 3
03.13.08 Transmission and Storage Confidentiality Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.	Y	Y	IPSec and encryption at rest. 2FA VPN to access summit.
03.13.09 Network Disconnect Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.	Y	Y	We terminate connections after 24 hours
03.13.10 Cryptographic Key Establishment and Management Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	Y	Y	

03.13.11 Cryptographic Protection Implement the following types of cryptography to protect the confidentiality of CUI: [Assignment: organization-defined types of cryptography].	Y	Y	Disk encryption OS level and AES-256 on the wire.
03.13.12 Collaborative Computing Devices and Applications a. Prohibit the remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]. b. Provide an explicit indication of use to users physically present at the devices.	Y	Y	This is our policy.
03.13.13 Mobile Code a. Define acceptable mobile code and mobile code technologies. b. Authorize, monitor, and control the use of mobile code.	Y	Y	Currently we have no mobile code
03.13.14 Withdrawn	W		Withdrawn in revision 3
03.13.15 Session Authenticity Protect the authenticity of communications sessions.	Y	Y	VPN and SSL/HTTPS connections are always used.
03.13.16 Withdrawn	W		Withdrawn in revision 3
3.14 SYSTEM AND INFORMATION INTEGRITY			
03.14.01 Flaw Remediation a. Identify, report, and correct system flaws. b. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates.	Y	Y	Critical vulnerabilities are dealt with within 24 hours.
03.14.02 Malicious Code Protection a. Implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code. b. Update malicious code protection mechanisms as new releases are available in accordance with configuration management policies and procedures. c. Configure malicious code protection mechanisms to: 1. Perform scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed; and 2. Block malicious code, quarantine malicious code, or take other mitigation actions in response to malicious code detection.	Y	Y	
03.14.03 Security Alerts, Advisories, and Directives a. Receive system security alerts, advisories, and directives from external organizations on an ongoing basis. b. Generate and disseminate internal system security alerts, advisories, and directives, as necessary.	Y	Y	Handled by the ISO
03.14.04 Withdrawn	W		Withdrawn in revision 3
03.14.05 Withdrawn	W		Withdrawn in revision 3
03.14.06 System Monitoring a. Monitor the system to detect: 1. Attacks and indicators of potential attacks and 2. Unauthorized connections. b. Identify unauthorized use of the system. c. Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.	Y	Y	Observability system
03.14.07 Withdrawn	W		Withdrawn in revision 3
03.14.08 Information Management and Retention Manage and retain CUI within the system and CUI output from the system in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	Y	Y	DMTN-199 is the only applicable source.
3.15. Planning			
03.15.01 Policy and Procedures a. Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI. b. Review and update policies and procedures [Assignment: organization-defined frequency].	Y	Y	

03.15.02 System Security Plan a. Develop a system security plan that: 1. Defines the constituent system components; 2. Identifies the information types processed, stored, and transmitted by the system; 3. Describes specific threats to the system that are of concern to the organization; 4. Describes the operational environment for the system and any dependencies on or connections to other systems or system components; 5. Provides an overview of the security requirements for the system; 6. Describes the safeguards in place or planned for meeting the security requirements; 7. Identifies individuals that fulfill system roles and responsibilities; and 8. Includes other relevant information necessary for the protection of CUI. b. Review and update the system security plan [Assignment: organization-defined frequency]. c. Protect the system security plan from unauthorized disclosure.	Y	Y	a. RTN-082 b. review at least annually c. this is considered a public document
03.15.03 Rules of Behavior a. Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI. b. Provide rules to individuals who require access to the system. c. Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system. d. Review and update the rules of behavior [Assignment: organization-defined frequency].	V	Y	Need new AUP
3.16. System and Services Acquisition			
03.16.01 Security Engineering Principles Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization- defined systems security engineering principles].	Y	Y	See RTN-082 Section 2.15
03.16.02 Unsupported System Components a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer. b. Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.	Y	Y	We keep uptodate and licensed.
03.16.03 External System Services a. Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements]. b. Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers. c. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.	Y	Y	a. No external providers are used for sensitive information.
3.17. Supply Chain Risk Management			
03.17.01 Supply Chain Risk Management Plan a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency]. c. Protect the supply chain risk management plan from unauthorized disclosure.	N	W	Not applicable for this project.
03.17.02 Acquisition Strategies, Tools, and Methods Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.	N	W	Not applicable for this project.
03.17.03 Supply Chain Requirements and Processes a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes. b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization- defined security requirements].	N	W	Not applicable for this project.
Total NIST800-171 requirements		**98**	
Total Rubin Intends to comply fully with		**94**	
Total Rubin Complies with in 2024		**84**	
Total Rubin waivers requested		**4**	
Total Rubin variances in 2024		**5**	

B References

[SQR-041], Allbery, R., 2022, *Science Platform security risk assessment*, SQuaRE Technical Note SQR-041, Vera C. Rubin Observatory, URL https://sqr-041.lsst.io/

[SITCOMTN-076], Bechtol, K., on behalf of the Rubin Observatory Project Science Team, S.R., 2025, *Information Sharing during Commissioning*, Commissioning Technical Note SITCOMTN-076, Vera C. Rubin Observatory, URL https://sitcomtn-076.lsst.io/

[NIST.FIPS.200], Division, C.S., 2006, Publication 200, minimum security requirements for federal information and information systems, URL https://doi.org/10.6028/NIST.FIPS.200

[RTN-073], Dubois, R., 2024, *Rules of Engagement for Accessing Data During the Embargo Period*, Technical Note RTN-073, Vera C. Rubin Observatory, URL https://rtn-073.lsst.io/

[RTN-072], Guy, L., 2024, *Rubin Operations Change Control Process*, Technical Note RTN-072, Vera C. Rubin Observatory, URL https://rtn-072.lsst.io/

[ACP], Marshall, P., 2024, *Access Control Plan for the Vera C. Rubin Observatory U.S. Data Facility Embargo Rack* , Tech. Rep. ACP, SLAC, URL https://ls.st/ACP,
Internal document

[DMTN-286], O'Mullane, W., Economou, F., 2024, *Data security for Rubin communication channels*, Data Management Technical Note DMTN-286, Vera C. Rubin Observatory, URL https://dmtn-286.lsst.io/

[DMTN-199], O'Mullane, W., Allbery, R., AlSayyad, Y., et al., 2024, *Rubin Observatory Data Security Standards Implementation*, Data Management Technical Note DMTN-199, Vera C. Rubin Observatory, URL https://dmtn-199.lsst.io/

[RTN-030], O'Mullane, W., Allbery, R., Dubois, R., Lim, K., 2024, *Rubin Data and Information Security Plan*, Technical Note RTN-030, Vera C. Rubin Observatory, URL https://rtn-030.lsst.io/

[RDO-71], Roberts, A., Blum, R., Claver, C., et al., 2024, *Rubin Observatory Risk and Opportunity Management Plan*, Data Management Operations Controlled Document RDO-71, Vera C. Rubin Observatory, URL https://rdo-71.lsst.io/

[NIST.SP.800-171r3], Ross, R., Pillitteri, V., 2024, Special publication 800-171, protecting controlled unclassified information in nonfederal systems and organizations, URL https://doi.org/10.6028/NIST.SP.800-171r3

[ITTN-074], Silva, C., 2024, *Pixel Zone Technology Control Plan*, Information Technology Technical Note ITTN-074, Vera C. Rubin Observatory, URL https://ittn-074.lsst.io/

[ITTN-070], Silva, C., Hoblitt, J., 2023, *Rubin Observability Project*, Information Technology Technical Note ITTN-070, Vera C. Rubin Observatory, URL https://ittn-070.lsst.io/

[ITTN-045], Tapia, D., Silva, C., 2024, *Summit Onboarding Procedure*, Information Technology Technical Note ITTN-045, Vera C. Rubin Observatory, URL https://ittn-045.lsst.io/

[ITTN-010], Thebo, A., Hoblitt, J., 2023, *User Identification and Authorization*, Information Technology Technical Note ITTN-010, Vera C. Rubin Observatory, URL https://ittn-010.lsst.io/

C Acronyms

Acronym	Description
AAA	Authentication, Authorization and Accounting
AC	Access Control
AES	Advanced Encryption Standard
AT	Awareness and Training
AU	Audit and Accountability
AURA	Association of Universities for Research in Astronomy
CA	Certification, Accreditation, and Security Assessments
CCB	Change Control Board
CM	Configuration Management
CP	Contingency Planning
CUI	Controlled Unclassified Information
DM	Data Management
DMTN	DM Technical Note
DWDM	Dense Wave Division Multiplex
EOL	End of Life
IA	Identification and Authentication

IPA	FreeIPA - Identity, Policy, Audit
IR	Incident Response
ISO	Information Security Officer
IT	Information Technology
ITTN	IT Technote
LHN	long haul network
MA	Maintenance
MAC	Media Access Control
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology (USA)
NOIRLab	NSF's National Optical-Infrared Astronomy Research Laboratory; `https://noirlab.edu`
NSF	National Science Foundation
OPS	Operations
OS	Operating System
PE	Physical and Environmental Protection
PL	Planning
PS	Personnel Security
PZ	photo-z
RA	Risk Assessment
RTN	Rubin Technical Note
S3	(Amazon) Simple Storage Service
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
SLAC	SLAC National Accelerator Laboratory
SOC	Security Operations Centre
SP	Story Point
SQR	SQuARE document handle
SSID	Service Set Identifier
SSL	Secure Sockets Layer
USB	Universal Serial Bus
USDF	United States Data Facility
UTC	Coordinated Universal Time

VPN	virtual private network
VRO	(not to be used)Vera C. Rubin Observatory