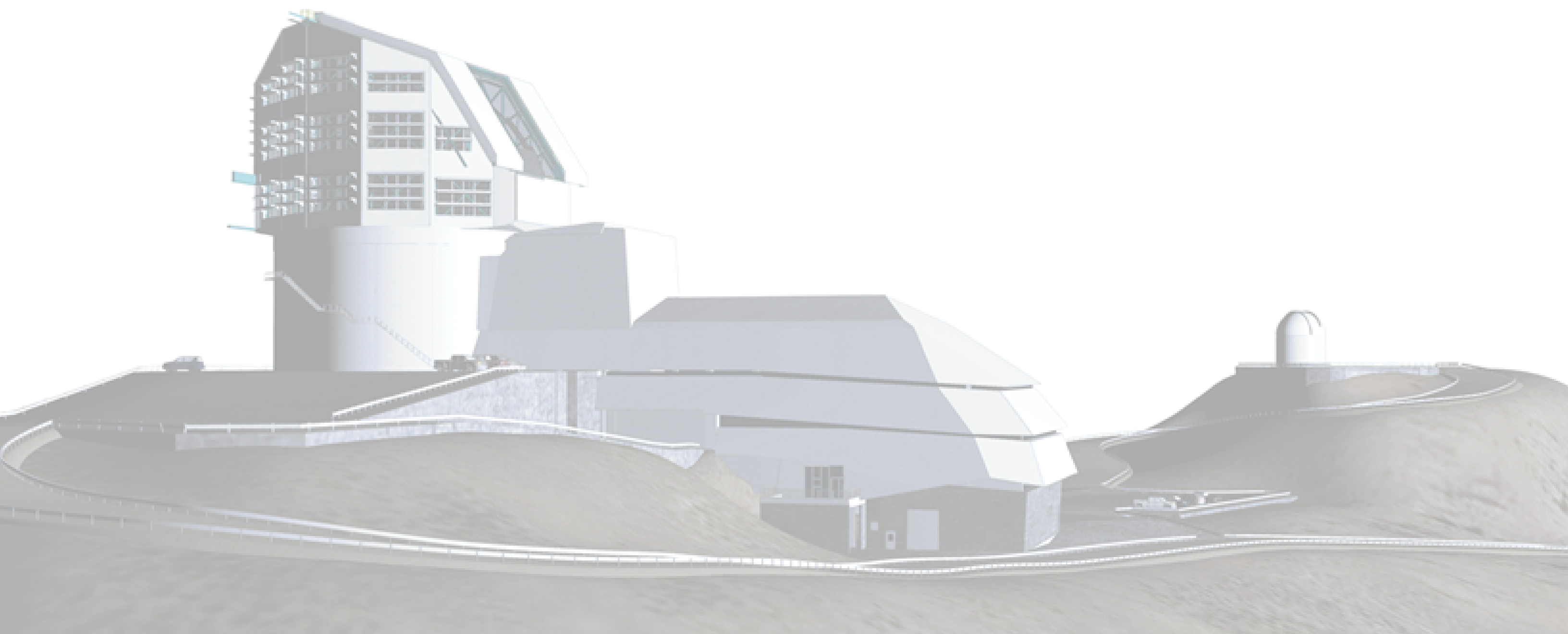
Vera C. Rubin Observatory
Data Management

Rubin Observatory Data Security Standards Implementation

William O'Mullane, Russ Allbery, Yusra AlSayyad, Eric Bellm, Andy Clements, Richard Dubois, Joshua Hoblitt, Cristián Silva, Ian Sullivan, Kian-Tat Lim

DMTN-199

Latest Revision: 2022-08-08



Abstract

In this document we describe a set of measures that we plan to take, in order to secure the data taken at Rubin Observatory to the standards set by the US funding agencies.

Change Record

Version	Date	Description	Owner name
0.1	2021-07-19	Unreleased. Set up structure	William O'Mullane
0.2	2021-09-28	Unreleased. First draft for JSR 2021	William O'Mullane
0.3	2021-10-04	Unreleased. Second draft for JSR 2021	William O'Mullane
0.4	2021-10-05	Unreleased. Tidy for JSR 2021	William O'Mullane
0.5	2021-11-23	Unreleased. Fix router price, inclide Huawei Avoid	William O'Mullane
1.0	2022-02-02	Remomved Huawei from this plan and added descriptions	Victor Krabbendam
1.1	2022-08-02	Simplify summary in intro	William O'Mullane

Document source location: `https://github.com/lsst-dm/dmtn-199`

Contents

Rubin Observatory Data Security Standards Implementation

1 Introduction

The agencies have provided a set of requirements for data security which are addressed in this upgrade plan. This document addresses the upgrades specifically and will augment the overall security plan for Rubin observatory (see LDM-324).

The requirements can be organized and summarized at a high level as follows :

1. Encrypt data following National Institute of Standards and Technology (USA) (NIST) .
2. Use firewalls to prevent unauthorized access.
3. Hold focal plane scientific data for a few days following the observation. Hold engineering and commissioning imaging data for several weeks.
4. Do not alert on artificial Earth-orbiting satellites. In order to do this, check some alerts against appropriate satellite catalogs.
5. Publish the survey schedule 24 hours in advance.
6. Request approval to observe without sidereal tracking.

Section 3 provides a subsection response for each of these bullets.

2 Cost Summary

A summary of the costs associated with implementing these enhanced security measures are summarized in Table 1 below. The table includes both non-recurring, up-front, costs as well as the costs to operated with these enhanced measures for a 10-year operation period.

Table 1: Cost Sumary Table for Enhance Security Requirements.

Item	Construction Cost	Operations Cost
Encryption (Table 2)	$2,124,000	$2,724,000
Firewalls and physical security (Table 3)	$1,428,624	$4,800,000
Delayed Data Store (Table 4)	$800,000	$800,000
Alert Vetting System (Table 5) ROP value		$13,662,042
Total Construction	**$4,352,624**	
Total Operations Cost		**$21,986,042**

Execution of this plan will begin immediately upon approval to complete the changes prior to data collection in the system commissioning phase of Construction.

3 Response to the requirements

This plan follows the applicable elements of NIST.SP.800-171. The application of this standard to the Rubin Observatory requires some interpretation. A compliance matrix is provided in Appendix A. In this matrix and in this document we assume the requirements apply to embargoed images before release to the collaboration and the derived difference image sources. Hence it applies to Prompt Processing, the embargoed data store(s), and the summit in Chile. It does not apply to DACs nor the actual alert stream.

The non-recurring costs in this plan include necessary end-equipment to manage the data entering the USDF. The incrimental operating costs at the USDF, expecting that they too will follow NIST 800-171, are provided in this document as reference.

From Section 2.1 of NIST.SP.800-171 we note that the confidentiality impact value for the data is no less than moderate. So we may assume our NIST.FIPS.200 security category would be { moderate, low, low}[1].

[1] {confidentiality, availability, integrity}

3.1 Encrypt Data

As outlined in DMTN-108 we shall buy four routers which can perform Internet Protocol Security (IPsec) AES-256 bit encryption between Chile and SLAC. We will not transfer embargoed images to France - hence we should keep a secure data store at Chile and at SLAC National Accelerator Laboratory (SLAC) for redundancy. The router cost in Table 2 is based on a quotation from Cisco as one of the vendors explicitly specified in the agency document. While we have shown that Transport Layer Security (TLS) with AES-256 can provide sufficient performance to meet our Alert timing budget, we have not yet measured performance with the specified routers using IPsec. We assume that performance will be adequate.

NIST also suggests out of band access - an independent network for access to the Summit systems in case the main network is down. A quote for Telconor to give a backup control link is included in Table 2.

See Table 2 for the cost breakdown. The Out Of Bound (Alternative network access) (OOB) access is in Chile only and the routers and cabling are an even split.

Table 2: This table provides cost estimates for encrypted data transfer.

Item	Cost	number	Total	Notes
Cisco Router (2@Chile 2@USDF)	$500,000	4	$2,000,000	Cisco quote
Cabling	$1,000	4	$4,000	
Out of Bounds (OOB) link install (Chile)	$60,000	2	$120,000	Times 2, we need summit-base and base-internet
Total Construction			**$2,124,000**	
OOB Ops running cost/month	$3,000	240	$720,000	
Router rehresh			$2,000,000	
Cabling	$1,000	4	$4,000	
Total Operations			**$2,724,000**	

3.2 Install Firewalls and other physical security devices

This requirement is for physical and cyber security. It includes installing cameras and locks on racks. Some of this such as Firewalls is already in the project plan but much of it is not.

Items already in the baseline include:

- Card access to server rooms.
- Backup network in case main link fails (though the microwave link is a new addition ..)
- Auditable process to handle onboarding/offboarding

- Some cameras are in the project but not complete coverage.

The firewalls and physical security will be upgraded to meet the enhanced standard. Table 3 includes the items needed for this upgrade.

Important Note: We shall ring fence the Camera in its own firewall with more restricted access than the restricted control network. However we will treat it as a black box deliverable for this requirement. We shall not expect encryption of the internal disks of the camera system. Any perturbation to the camera system will have a deleterious effect on the camera with significant development and schedule impacts.

Signage and labeling, as required in NIST 171 3.8.4 [2], will be developed as appropriate.

NIST 1.7.1 Section 3.10.6 pulls in extra standards for remote work namely NIST.800-46 and NIST.800-114. NIST.800-114 is the broader scope and we are pretty much in line with how it is written - we note Section 5.2.1 that we use Onepassword as a vault for Information Technology (IT) passwords - not paper in a fire proof safe as recommended. Some other suggestions are understood to be useful in general but often not suitable for developers - personal firewalls, application filtering and aggressive antivirus software often trip over developer code and tools.

NIST.800-46 and other related NIST documentation suggest threat modeling - we do this in a limited way e.g SQR-041 and SQR-037. A more exhaustive risk assessment by a third party is not anticipate at this time but the Project team will discuss with SLAC on any plans to review the United States Data Facility (USDF). We do not store sensitive information on the virtual private network (VPN) nor bastion nodes. We do use Network Address Translation (NAT) in a limited number of places - this will be more important in operations if/when we move to IPv6.

Table 3: This table provides cost estimates for firewalls and other physical security in Chile and at SLAC not in the project plan.

Item	Cost	number	Total	Notes
Locks USDF	$200	30	$6,000	
Cameras Detectors USDF	$2,000	1	$2,000	
Sensors USDF	$38	30	$1,140	https://www.server-rack-online.com/ig-dsw-2m.html
Sensor hub USDF	$448	1	$448	https://www.server-rack-online.com/ec-300m.html
Locks Chile	$200	30	$6,000	1 set has 2 locks, front and back, https://www.apc.com/shop/in/en/products/Combination-Lock-Handles-Qty-2-for-NetShelter-SX-SV-VX-Enclosures/P-AR8132A
Cameras Detectors Chile	$2,000	2	$4,000	
Sensors Chile	$38	30	$1,140	
Sensor hub Chile	$448	2	$896	https://www.server-rack-online.com/ec-300m.html

[2] https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf

Faster CPU to handle disk encryption on summit (node price)	$13,000	20	$260,000	sizing model rome price
SSD price differnce to SATA (cost/TB)	$250	260	$65,000	from sizing model NVMe price
Labor to redeploy all summit systems (contract)	$100	1,200	$120,000	Hey Siri FaceTime
Labelling and signage	$2,000	1	$2,000	https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf
Security related contracts/month	$40,000	24	$960,000	
Total Construction			**$1,428,624**	
Operations Security contracts	$40,000	120	$4,800,000	
Total Operations			**$4,800,000**	

This enhanced security plan includes support from an outside security provider. It is estimated running an Security Operations Centre (SOC) could cost upward of $1.4M per year[3]. This article[4] outlines the pros and cons of an outsourced SOC and estimates it at between 300 and 800K per year. For budgeting purposes $40K a month is included in Table 3. Such a contract (or contracts) should cover:

1. Proactive monitoring and alerting (NIST 171 section 3.3.5)
    - Write alerts for suspicious behaviors
    - Analyze collected logs for anomalies
2. Root cause analysis of any alert or anomaly
3. Incident response
    - Isolation of attacker
    - Forensic analysis leading to timeline and inventory of compromise
    - Identifying systems that will need to be rebuilt
4. Vulnerability scanning including filtering out false positives
5. Asset inventory including patch status
6. Penetration testing to proactively look for vulnerabilities

This will require extensive coordination and integration with existing IT services and processes, included as part of this cost.

[3]https://expel.io/blog/how-much-does-it-cost-to-build-a-24x7-soc/
[4]https://www.linkbynet.com/outsourced-soc-vs-internal-soc-how-to-choose

Since we will have to encrypt systems on the summit (see ITTN-014) for a list of systems) we anticipate upgrade processors and solid state drives (Solid-State Disk (SSD)) are required. Determining the detailed specifications will require experimentation so the values in the table for this are engineering estimates.

Note that compute facilities for the Commissioning Cluster at the Base as well as Alert Production and the Staff RSP at the USDF are not considered to be within the physical security area. Rubin considers the short-term, ephemeral processing on these resources outside of the enhanced security requirmenets. Including them would approximately double the cost of this item for Construction.

3.3 Delay public release

Rubin considers the best approach to managing public release of data is to keep the embargoed data on a secure device separate from other systems and migrate images to the regular repository as they become *public*. This can be an object store with encryption like MinIO [5]. We will need to have one at SLAC and one at Chile for redundancy to ensure no data loss.

With the commissioning constraint that means this needs to be approxemately a one month store for full images and engineering data. Looking at DMTN-135 table 40 this comes out to about 500TB of usable disk. Table 4 gives the cost calculation or this.

The nominal embargo for regular operations we understand as between a few days (most images) and ten days (some images as specified by Alert Vetting).

Table 4: This table provides costs for the embargoed data store.

Description	**value**	
Number of days data to store	30	
Raw data size per day (TB compressed)	16	Years data from Table 40 of DMTN-135/ 298.3 observing nights (Key Numbers Confluence)
Useable size needed (TB)	484	
Allowing for RAID (TB)	1000	
Cost for 1 store	$400,000	Using SLAC Fast Disk Price from Table 28 of DMTN-135
Total for 2 stores - Construction	**$800,000**	
Total Ops Cost at least 1 Refresh	**$800,000**	

Note: To enact these enhanced security measures on Commissioning data, this plan focuses on early data processing at the SLAC USDF and not the resources originally planned at NCSA. The SLAC USDF must be ready with sufficient services and capacity for ComCam, on sky work.

[5] `https://min.io/product/enterprise-object-storage-encryption`

Figure 1 depicts the encrypted storage and network. Embargoed (delayed) data would be held in the encrypted stores for the time specified. We assume temporary processing for alerts does not have to be encrypted, NIST allows ephemeral unencrypted data for processing.

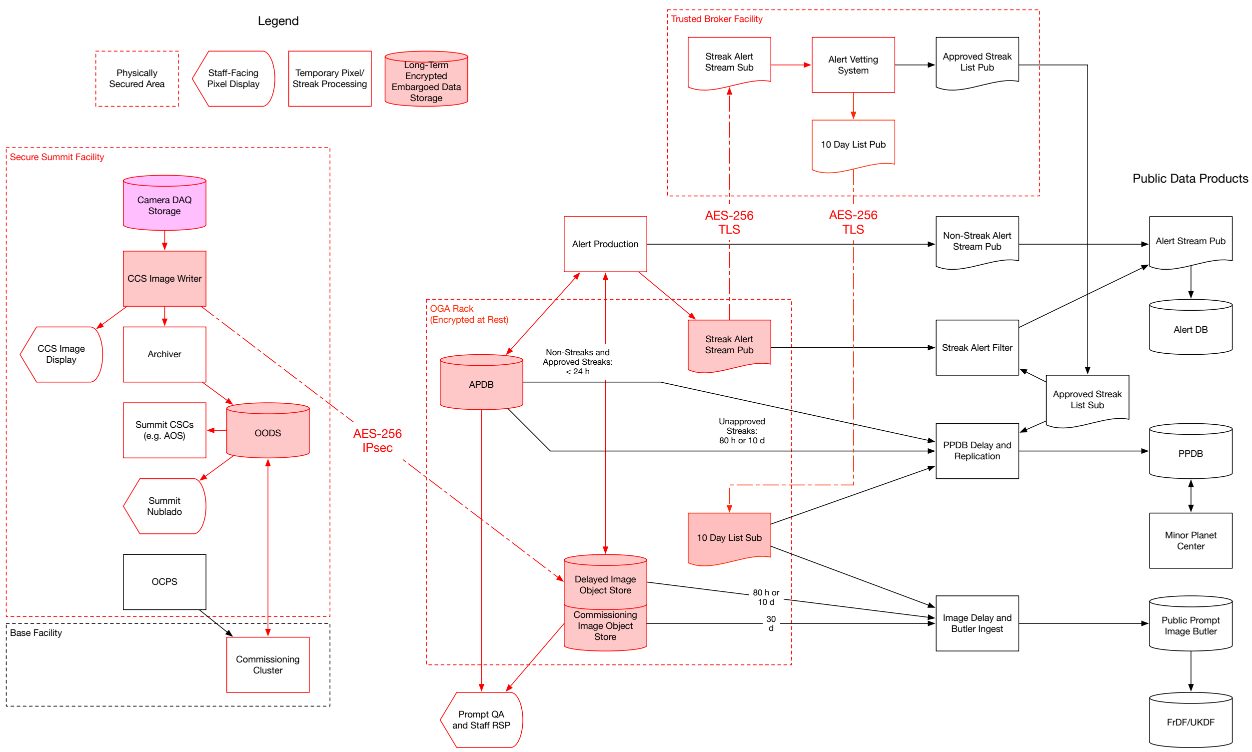


FIGURE 1: OGA architecture showing the long term encrypted storage and encrypted network from Chile to SLAC.

3.4 Eliminate earth orbiting satellites

Rubin does not publish alerts for streaks associated with artificial satellites. A subset of streaks, potentially consistent with Earth-orbiting satellites or Solar System objects, will be evaluated by the Alert Vetting System (AVS). AVS is under discussion currently in terms of design and how it may be implemented. The cost here is based on FTE and non labor after initial discussions with Lawrence Livermore National Laboratory (LLNL). They are assuming a high availability service. An estimate is given in Table 5. This also includes the current value in the operations plan. The cost of delaying the data in an encrypted store is already covered in Section 3.3

Table 5: The Alert Vetting System is all FTE cost - apart from unknown hardware at LLNL.

Description	Cost	Count	Total
FTE per year	$416,000	2.6	$1,081,600
Mission years		10	$10,816,000
Pre operations years	$1,000,000	2	$2,000,000
non labor 1 off	$611,000	1	$611,000

non labor recurring	$25,000	10	$250,000
Total			**$0**
Rubin Operations Plan Value			$13,662,042

3.5 Alert Verification

This is under discussion with LLNL - initial cost estimates are given in Section 3.4. It is shown in Figure 1.

3.6 Publish nominal schedule

The project was already planning to publish the observing schedule to allow co observing of sources, see Section 2.1 of LSE-30. The Observatory System Specifications; LSST Systems Engineering (Document Handle) (LSE)-30 (OSS) requires publication at least two hours ahead of observing - the request here is to have the schedule twenty four hours in advance. This is not a problem as long as one understands the fidelity of the schedule decreases with the look ahead time. The agency requirement acknowledges this.

The schedule is to be delivered to the trusted broker - we shall arrange this with LLNL.

We consider no delta cost for this as it was in the project plan.

3.7 Request approval for non sidereal tracking

This is best handled Procedurally and as such will not produce a delta cost on the project.

4 Conclusion

We can comply with the requirements and NIST 1.7.1 at the cost outlined in Section 2.

There are a few assumptions explicitly made above which we feel comply with given requirements but did require interpretation. To be explicit:

- Section 3 Assumes embargoed images before release to the collaboration are treated securely. After the embargo is lifted there is no longer a need to secure the images at the higher requirements.

- Section 3 Assumes NIST 1.7.1 also applies to SLAC even though NIST.FIPS.200 should be applicable.
- Section 3.2 Makes an important note about *not encrypting* internal camera storage.
- Section 3.2 Assumes NIST.800 documents were written as guidance they will be noted but we may not always follow all recommendations in all cases.
- Section 3.3 Assumes the embargo for commissioning applies to use of encrypted storage and transfers. This potentially implies National Center for Supercomputing Applications (NCSA) could not be used for commissioning at all.
- Section 3.2 and Section 3.3 Assumes short stays of data on unencrypted machines for processing is ok (it is in line with NIST).

A Compliance with NIST Standard

Table 6: This table provides an overview of the NIST.SP.800-171 and Rubin compliance with it.

NIST 800-171	2021 Status	Intended Compliance	Note
3.1 ACCESS CONTROL			
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Y	Y	
3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	N	Y	There are many non-administrative users with unrestricted sudo access, this will be addressed.
3.1.3 Control the flow of CUI in accordance with approved authorizations.	Y	Y	
3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	N	Y	Principle of least privilege is applied. Many users have access to hosts that is unneeded.
3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.	N	Y	Targeted sudo rules are needed for common operations. IPA controls sudo centrally
3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.	Y	Y	
3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.		Y	This is probably sudo attempts audits. Full commands can be logged in at the cost of extra load for the servers.
3.1.8 Limit unsuccessful login attempts.	N	Y	Web Services such as love, foreman, ipa console, nublado, etc. may need rate limiting. We dont use passwords in ssh hosts only ssh keys which many conisder more secure - we are not aware of a retry limit for ssh-key access, an approriate extra security would be to not use the default port 22. However, we do limit attemtps to 6 with a block of 600 minutes, this will efectively block failed SUDO logins.
3.1.9 Provide privacy and security notices consistent with applicable CUI rules.	N	Y	Check login notices etc. A login banner can be displayed upon login
3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	Y	Y	This is our policy.
3.1.11 Terminate (automatically) a user session after a defined condition.	N	Y	ssh sessions are generally not limited on hosts; some network equipment has timeouts set; nublado has a session limit for notebooks?
3.1.12 Monitor and control remote access sessions.	N	Y	We currently check who and from where is connecting.
3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Y	Y	VPN is in use
3.1.14 Route remote access via managed access control points.	N	Y	Bastion nodes – LHN is an open back door with no ACLs
3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.	Y	Y	
3.1.16 Authorize wireless access prior to allowing such connections.	Y	Y	All devics attaching in Chile need to be registered by Mac address.
3.1.17 Protect wireless access using authentication and encryption.	Y	Y	
3.1.18 Control connection of mobile devices.	Y	Y	In the sense there is no open wifi, and on the summit devices must be registered.
3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23	Y	Y	Data will not exist on mobile devices - in the case where an image may exist on say commissioning team laptop we will have disk encryption enabled.
3.1.20 Verify and control/limit connections to and use of external systems.	Y	Y	This implies vetting of devices that connect to the control network - we use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the long haul network (LHN) Service Set Identifier (SSID) and Virtual Local Area Network (VLAN)s.
3.1.21 Limit use of portable storage devices on external systems.	N	Y	Can be rolled out with puppet but there are some servers that need usb.
3.1.22 Control CUI posted or processed on publicly accessible systems.	Y	Y	We do not intend to post images on publicly accessible systems.
3.2 AWARENESS AND TRAINING			
3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	Y	Y	
3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	N	Y	
3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Y	Y	We would like to do more here like capture flag exercises for developers or blue/red teams events
3.3 AUDIT AND ACCOUNTABILITY			
3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	Y	Y	
3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.	Y	Y	

3.3.3 Review and update logged events.	P	Y	We may look for a third party contract for this.
3.3.4 Alert in the event of an audit logging process failure.	N	Y	
3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	N	Y	Again shall look for third party contract for this
3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.	N	Y	
3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records.	Y	Y	
3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Y	Y	
3.3.9 Limit management of audit logging functionality to a subset of privileged users.	Y	Y	
3.4 CONFIGURATION MANAGEMENT			
3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Y	Y	We use mainly infrastructure as code approaches so the software is well tracked. IT inventory all the hardware.
3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.	Y	Y	
3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.	Y	Y	We have CCBs and code change process in place which also cover the infrastructure as code.
3.4.4 Analyze the security impact of changes prior to implementation.	Y	Y	
3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	Y	Y	
3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	N	Y	
3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	Y	Y	We get a lot of this by mainly containerizing the applications and having users work within deployed containers.
3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	N	Y	We need to implement SUDO lists to restrict access. However, this could be related to blacklisting of applications.
3.4.9 Control and monitor user-installed software.	Y	Y	
3.5 IDENTIFICATION AND AUTHENTICATION			
3.5.1 Identify system users, processes acting on behalf of users, and devices.	Y	Y	
3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	Y	Y	
3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	N	Y	Chile dont require 2FA at the moment
3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non- privileged accounts.		Y	Chile dont require 2FA at the moment, but certificates are deployed to prevent mitm
3.5.5 Prevent reuse of identifiers for a defined period.	N	Y	
3.5.6 Disable identifiers after a defined period of inactivity.	Y	Y	
3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.	Y	Y	
3.5.8 Prohibit password reuse for a specified number of generations.	Y	Y	
3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.	Y	Y	
3.5.10 Store and transmit only cryptographically-protected passwords.	Y	Y	
3.5.11 Obscure feedback of authentication information.	Y	Y	
3.6 INCIDENT RESPONSE			
3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Y	Y	AURA have insurance which covers this. But we really should have a contract to look over logs etc. to note when we are hit.
3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Y	Y	
3.6.3 Test the organizational incident response capability.	N	Y	
3.7 MAINTENANCE			
3.7.1 Perform maintenance on organizational systems.	Y	Y	
3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	Y	Y	
3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Y	Y	
3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	Y	Y	
3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	N	Y	Chile dont do 2FA yet. 2 factor authentication system (Duo) has the capability to kill sessions.
3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.	Y	Y	
3.8 MEDIA PROTECTION			

3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	N	Y	
3.8.2 Limit access to CUI on system media to authorized users.	N	Y	
3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.	Y	Y	
3.8.4 Mark media with necessary CUI markings and distribution limitations.	N	Y	We understand we should label rooms and machines acording to https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf
3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	Y	Y	
3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	N	Y	
3.8.7 Control the use of removable media on system components.		Y	Can be rolled out with puppet but there are some servers that need usb.
3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.	Y	Y	
3.8.9 Protect the confidentiality of backup CUI at storage locations.	Y	Y	
3.9 PERSONNEL SECURITY			
3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.	Y	Y	Only project team members will have access to early images - all are know individuals. This doesn't suggest background security screening and it was also explicitly not required by the agencies in section 2 of the requirements document.
3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Y	Y	
3.10 PHYSICAL PROTECTION			
3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	Y	Y	This physical access limitations will increase with locks on server cabinets etc. but key card access is already in place.
3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.	Y	Y	Security is in place on Cero Pachon and at the entrance to the mountain - though not only for Rubin so not permanently at the observatory.
3.10.3 Escort visitors and monitor visitor activity.	Y	Y	Actual visitors are escorted on the summit - contractors are considered more like staff.
3.10.4 Maintain audit logs of physical access.	N	Y	Chile use Noirlab key-card system, we should reach to them to inquire about their audit procedures
3.10.5 Control and manage physical access devices.	Y	Y	
3.10.6 Enforce safeguarding measures for CUI at alternate work sites.	Y	Y	This brings in NIST.800-46 and NIST.800-114. Threat analysis suggested. NAT considered bad.
3.11 RISK ASSESSMENT			
3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	Y	Y	
3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	N	Y	Third party contract
3.12 SECURITY ASSESSMENT			
3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Y	Y	
3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Y	Y	
3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Y	Y	
3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	N	Y	Like any documentation this security documentation can get out of date.
3.13 SYSTEM AND COMMUNICATIONS PROTECTION			
3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	Y	Y	
3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	Y	Y	We can do more here.
3.13.3 Separate user functionality from system management functionality.	N	Y	This is difficult in development and commissioning but should be ok in operations.
3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.	N	Y	This will require training the operators and scientist who have access to the CUI data to not put it on their devices.

3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Y	Y	
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Y	Y	We may need to bring up iptables on each host
3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	Y	Y	
3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	N	Y	IPSec and encryption coming
3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Y	Y	
3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.	Y	Y	
3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	N	Y	
3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Y	Y	We should take care with the new roaming camera.
3.13.13 Control and monitor the use of mobile code.	Y	Y	Currently we have no mobile code
3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	N	Y	Chile dont monitor voip callls
3.13.15 Protect the authenticity of communications sessions.	Y	Y	
3.13.16 Protect the confidentiality of CUI at rest.	N	Y	
3.14 SYSTEM AND INFORMATION INTEGRITY			
3.14.1 Identify, report, and correct system flaws in a timely manner.	Y	Y	
3.14.2 Provide protection from malicious code at designated locations within organizational systems.	Y	Y	
3.14.3 Monitor system security alerts and advisories and take action in response.	Y	Y	
3.14.4 Update malicious code protection mechanisms when new releases are available.	Y	Y	
3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	Y	Y	
3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Y	Y	
Total requirements		**108**	
Total Rubin Intends to comply with		**108**	
Total Rubin Complies with in 2021		**72**	

B References

[SQR-037], Allbery, R., 2020, *SQuaRE security risk assessment*, SQR-037, URL `https://sqr-037.lsst.io/`,
Vera C. Rubin Observatory SQuaRE Technical Note

[SQR-041], Allbery, R., 2021, *Science Platform security risk assessment*, SQR-041, URL `https://sqr-041.lsst.io/`,
Vera C. Rubin Observatory SQuaRE Technical Note

[LSE-30], Claver, C.F., The LSST Systems Engineering Integrated Project Team, 2018, *Observatory System Specifications (OSS)*, LSE-30, URL `https://ls.st/LSE-30`

[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`

[ITTN-014], Gonzalez, I., 2022, *Computing Infrastructure*, ITTN-014, URL `https://ittn-014.lsst.io/`,
Vera C. Rubin Observatory

[LDM-324], Kantor, J., 2016, *Data Management Information Security Plan*, LDM-324, URL `https://ls.st/LDM-324`

[DMTN-108], O'Mullane, W., 2021, *Security of Rubin Observatory data*, DMTN-108, URL `https://dmtn-108.lsst.io/`,
Vera C. Rubin Observatory Data Management Technical Note

[DMTN-135], O'Mullane, W., Dubois, R., Butler, M., Lim, K.T., 2021, *DM sizing model and cost plan for construction and operations.*, DMTN-135, URL `https://dmtn-135.lsst.io/`,
Vera C. Rubin Observatory Data Management Technical Note

[NIST.SP.800-171], ROSS, R., VISCUSO, P., GUISSANIE, G., DEMPSEY, K., RIDDLE, M., 2020, Special publication 800-171, protecting controlled unclassified information in nonfederal systems and organizations, URL `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf`

[NIST.800-114], Souppaya, M., Scarfone, K., 2016, COMPUTER SECURITY, URL `https://doi.org/10.6028/NIST.SP.800-114r1`

[NIST.800-46], Souppaya, M., Scarfone, K., 2016, COMPUTER SECURITY, URL `https://doi.org/10.6028/NIST.SP.800-46r2`

C Acronyms