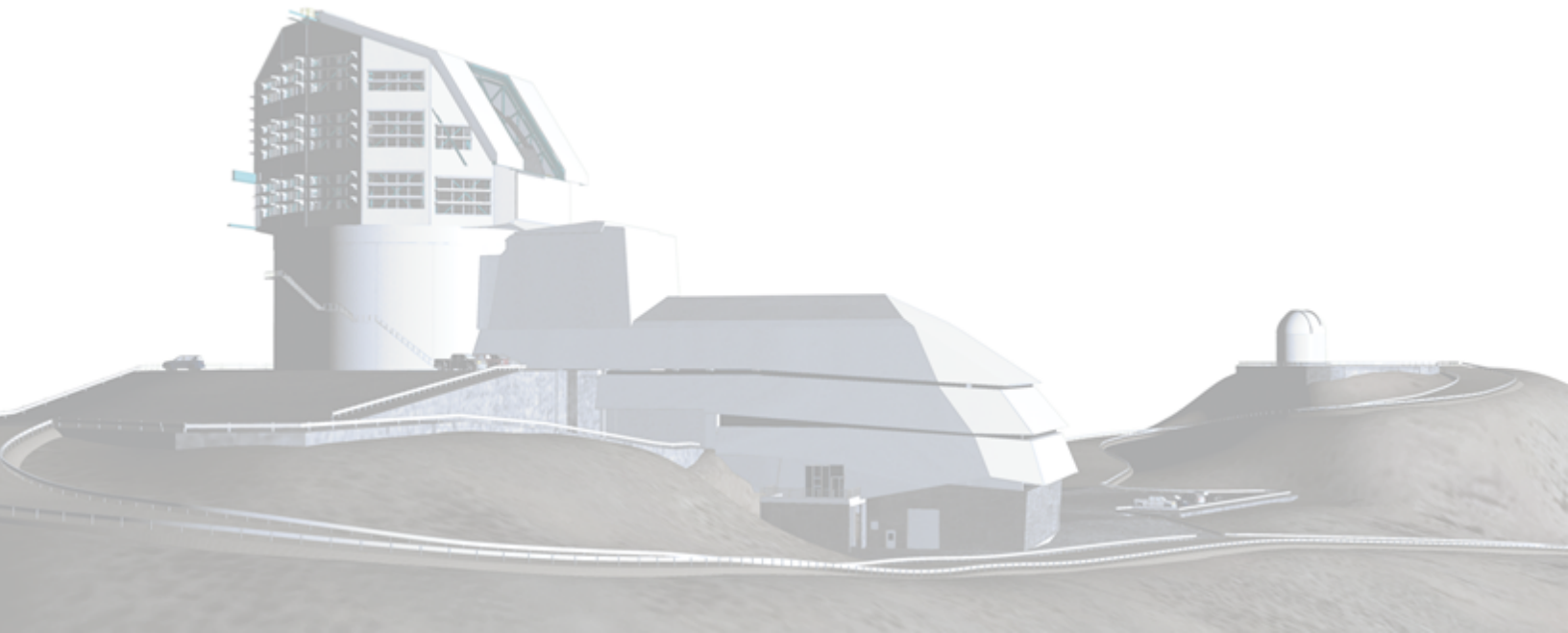
Vera C. Rubin Observatory
Data Management

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, Phil Marshall
Agency oversight: Ashley Zauderer-Vanderley (NSF), Helmut Marsiske (DOE)

DMTN-199

Latest Revision: 2024-09-01



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, include Huawei Avoid	William O'Mullane
1.0	2022-02-02	Removed Huawei from this plan and added descriptions	Victor Krabbendam
1.1	2022-08-02	Simplify summary in intro	William O'Mullane
1.2	2022-10-04	Include notes on working with commissioning data	Phil Marshall
1.3	2022-10-26	Embargo clarification	William O'Mullane
2.0	2023-06-08	Updated Requirements from NSF and DOE. Include agency oversight.	William O'Mullane, Bob Blum, Phil Marshall
2.1	2024-07-12	Removed mention of derivative catalogs	Phil Marshall
2.2	2024-08-02	Remove compliance appendix - point to RTN-082	William O'Mullane
2.3	2024-09-01	Make ComCam exemption explicit - tidy some embargo wording	William O'Mullane, Phil Marshall

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

Contents

Rubin Observatory Data Security Standards Implementation

1 Introduction

The funding agencies, National Science Foundation (NSF) and Department of Energy (DOE), 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 using strong, approved encryption standards, following NIST.SP.800-171r3 for Controlled Unclassified Information (CUI) at non federal organizations. The required use of these National Institute of Standards and Technology (USA) (NIST) security standards is limited to the physical security and encryption points. It does not extend to treating the data as CUI. The data should *not* be marked as CUI.
2. Use firewalls and physical security best practices to prevent unauthorized network access. Documented compliance shall be in accordance with NIST.SP.800-171r3.
3. Delay public release of focal plane scientific data for an embargo period of at least 80 hours following the observation. Hold engineering and commissioning imaging data for an embargo period of at least 30 days. Data aside from focal plane data may be made available following the original project plan which includes astronomical metadata (within 24 hours), standard postage stamp images (within 60 sec) not corresponding to artificial Earth-orbiting satellites (see Requirement 4), and weather and sky monitoring data. NSF and DOE require a system in place to extend the embargo times for the release of focal plane scientific data in the unlikely event that it is needed.
4. Eliminate artificial Earth-orbiting satellites. To do this, do not issue alerts on streaks that correspond to objects moving faster than 10 deg/day relative to sidereal tracking or for objects whose angular velocity cannot be determined. Additionally, any object in the appropriate catalogs provided to the U.S. Data Facility shall be eliminated from the Prompt Alert Stream and withheld from the publicly searchable Prompt Processing Database. SLAC shall handle any observations and/or ephemerides used to create and/or update

orbital elements in a satellite database or catalog as OFFICIAL USE ONLY and implement appropriate controls as directed by DOE.

5. Publish the nominal survey schedule 24 hours and an updated schedule at least 2 hours in advance. Once complete, publicly provide the actual executed observation. It is understood the schedule may change in real-time due to weather or other unforeseen circumstances.

6. Only observe without sidereal tracking in regions pre-approved by NSF and DOE. Currently, the only restrictions when operating in non-sidereal tracking modes include that no part of the field of view shall be within ± 2 degrees inclination of the Geosynchronous Earth Orbit (GEO) belt orbital plane. No camera bore sights shall be between $+1.0$ and $+9.0$ degrees of declination. Currently, no other bore sight restrictions are anticipated; however, NSF and DOE may add additional non-sidereal tracking field of view restrictions in the future.

The six requirements summarized above will be in place for the commissioning phase of the integrated Rubin Observatory system. Specifically, the requirements will pertain to data obtained with the LSST Camera in place on the telescope for commissioing and going forward into full survey operations. These added data security requirements in the present document do not apply to earlier phases of commissioing with the Commissioning Camera (also known as ComCam), nor to the data obtained in any phase at the Rubin Auxilliary Telescope (Auxtel).

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

As we approach the operations phase of Rubin Observatory and prepare to deliver data products to the community for the Legacy Survey of Space and Time, we want to remind the community of the basic data products delivered by alert production and data releases.

Nightly alert packets will be produced and streamed to community brokers at the 60 sec cadence (design specification, the minimum requirement is 120 sec), including postage stamps of size 32×32 pixels (6.4×6.4 sq. arcsec, or larger—for more details, please see LSE-63). A database of objects detected on difference images will be updated nightly and available through the Rubin Science Platform (Rubin Science Platform (RSP)). Following guidance from the funding agencies, full frame (3.2 Gpix) images in all three flavors (raw, calibrated, and difference), will be made available 80 hours after they were obtained. A small fraction of the total of all images obtained may be held longer than 80 hr and a mechanism for extending em-

bargo periods for certain images at the request of the funding agencies will be implemented. Rubin has consulted with scientists in the community and determined that the policy directive for this 80 hour delay will not significantly impact most science investigations. Additionally no prompt alerts will be issued for sources corresponding to objects in an appropriate satellite catalog. And no prompt alerts for streaks greater than 10 deg/day relative to sidereal. The exclusion of prompt alerts for these streaks will have minimal impact on science. In the rare event an unknown solar system object source with a streak length greater than 10 deg/day relative to sidereal potentially corresponds with ans earth impacting asteroid, the United States Data Facility (USDF) will implement a method to send any candidate impactors to the Minor Planet Center (MPC) during the embargo period. All data in transit shall comply with the strong, approved encryption standards outlined for the embargo period.

In addition, commissioning and engineering data will be embargoed for all non-commissioning team staff for 30 days. After this 30 day embargo, only with explicit approval may proprietary data products from commissioning be shared outside the Commissioning Team SITCOMTN-010.

Commissioning Team members are expected to use approved Project tools and processes for communication, data access and analysis, documentation, software development, work management, etc. In practice, we expect most work done by the Commissioning Team on the commissioning data to be done within private directories at the Rubin US Data Facility at SLAC.

Appropriate data and data products from commissioning will be assembled in data previews and released to the community within about 6 months of the end of the associated phase of commissioning (e.g, DP1 will be released approximately 6 months after the The commissioning camera is a single-raft, 9-CCD camera that will be installed in LSST during commissioning, before the final camera is ready. (ComCam) observations are completed). It is expected that a data preview based on science validation survey data from the ultimate phase of LSST Cam commissioning (about 2 months of Science Validation Surveys) will be made available early in full survey operations, before the first data release processing begins.

As per SITCOMTN-010, Rubin will define a process to approve the sharing of *derived data products* (see the Rubin Data Policy, RDO-013) based on commissioning data with the data rights holder community prior to the associated data preview release. This is needed to enable the Legacy Survey of Space and Time (formerly Large Synoptic Survey Telescope) (LSST) science

community to begin learning about Rubin data in preparation for their survey analyses.

Survey data releases including coadded images and updated source photometry will begin about one year after the start of the full survey. Our current plan is to acquire six months of data for the first formal LSST data release. Alert production will reach its full throughput and steady-state efficiency after Data Release 1; during the first survey year, alerts will be produced incrementally once adequate image templates are available (for more details, please see DMTN-107).

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
Satelite elimination(Table 5)		$3,815,000
Total Construction	**$4,352,624**	
Total Operations Cost		**$12,139,000**

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.800-171r3. The application of this standard to the Rubin Observatory requires some interpretation. A compliance matrix is provided in RTN-082. In this matrix and in this document we assume the requirements apply to embar-

goed 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.800-171r3 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].

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	

[1] {confidentiality, availability, integrity}

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.

Additional items may include locks on server racks, sensors and cameras to record the opening of cabinets, out of band channel for physical security alerts if the main network is disabled, and controls to prevent booting from USB devices or copying to external media.

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

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

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 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
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

[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

- 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.

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 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 requirements. 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.

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

With the commissioning constraint that means this needs to be approximately 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 to be 80 hours (all images). While not anticipated, the system includes the ability to embargo some images for longer periods of time at the request of the funding agencies.

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.

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.

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 determined by comparison with an appropriate catalog or catalogs at the USDF. Any object that corresponds to an object in this catalog will not be released in the prompt alerts or stored in the prompt alert database. SLAC will not create any catalogs with information corresponding to these objects. Additionally no streaks will be alerted on with a streak length greater than 10 deg/day relative to sidereal. In the rare event an unknown solar system object source with a streak length greater than 10 deg/day potentially corresponds with an Earth-impacting asteroid, SLAC shall implement a method to send any candidate impactors to the Minor Planet Center during the embargo period, complying with encryption standards for data in transit during the embargo period.

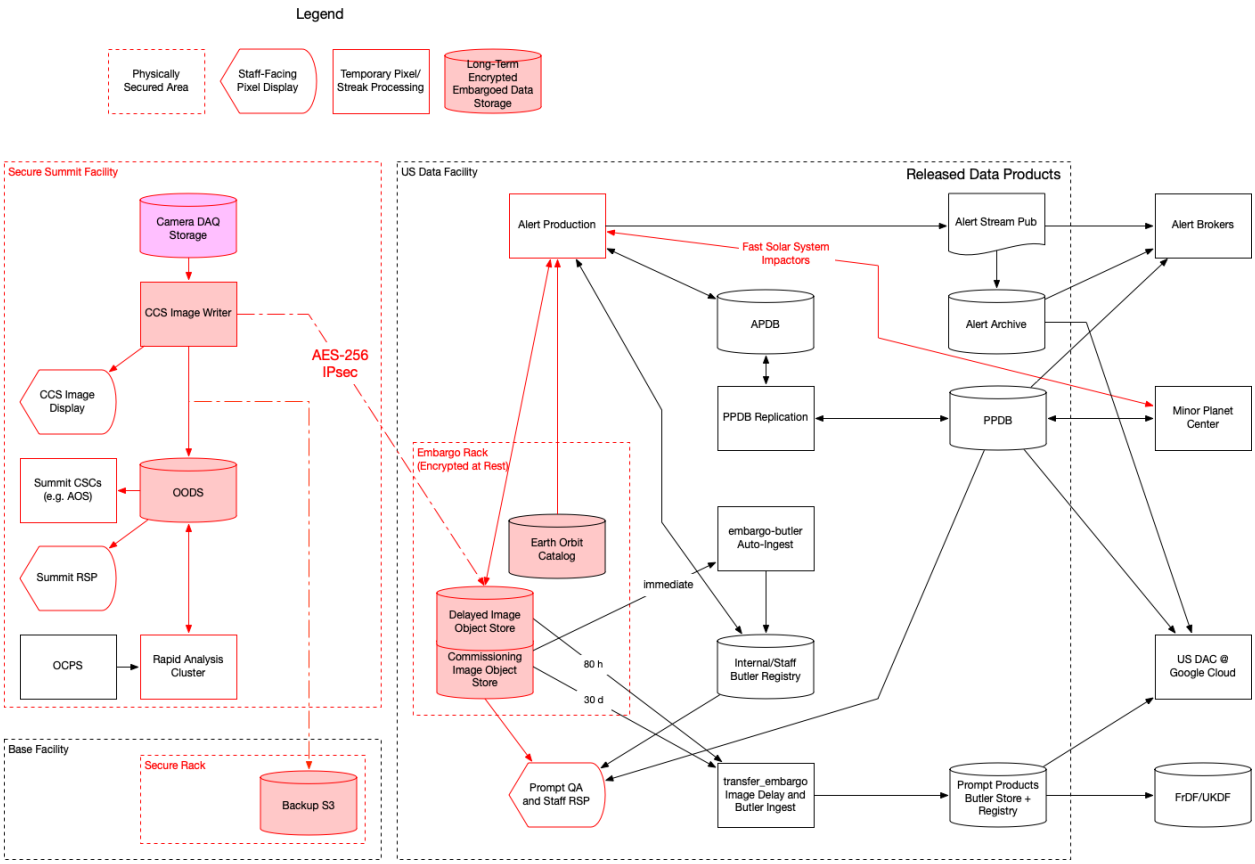


FIGURE 1: Architecture diagram showing many details including the long term encrypted storage and encrypted network from Chile to SLAC.

The estimated cost for this is based mainly on FTE - we do not consider the need for extra hardware unless the agencies wish for hardware encryption for the few occasions we need to send a secure message to MPC. 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 subsection 3.3

Table 5: The elimination of earth-orbiting satellites will require some Alert System modification which is all FTE cost.

Description	Cost	Count	Total
FTE per year (USDF Team, SLAC)	$345,000	0.5	$172,500
FTE per year (AP team)	$200,000	0.5	$100,000
Mission years		10	$2,725,000
Pre operations years (2 FTE)	$545,000	2	$1,090,000
Total			**$3,815,000**
Rubin Operations Plan Value (needs update)			$13,662,042

3.5 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 also published 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 publicly. The Project shall also publicly publish the executed observing plan.

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

3.6 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.
- subsection 3.2 Makes an important note about *not encrypting* internal camera storage.
- subsection 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.
- subsection 3.3 Assumes the embargo for commissioning applies to use of encrypted storage and transfers. This would imply embargoed data is only held at SLAC and in Chile.
- subsection 3.2 and subsection 3.3 Assumes short stays of data on unencrypted machines for processing is ok (it is in line with NIST).

A References

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

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

[SITCOMTN-010], Bechtol, K., Claver, C., Test, S.I., et al., 2021, Announcement of Opportunity: Community Engagement with Rubin Observatory Commissioning Effort, URL https://sitcomtn-010.lsst.io/,
Vera C. Rubin Observatory Commissioning Technical Note SITCOMTN-010

[RDO-013], Blum, R., the Rubin Operations Team, 2020, Vera C. Rubin Observatory Data Policy, URL https://ls.st/RDO-013,
Vera C. Rubin Observatory RDO-013

[LSE-30], Claver, C.F., The LSST Systems Engineering Integrated Project Team, 2018, Observatory System Specifications (OSS), URL https://ls.st/LSE-30,
Vera C. Rubin Observatory 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., Reinking, H., Silva, C., 2023, Computing Infrastructure, URL https://ittn-014.lsst.io/,
Vera C. Rubin Observatory ITTN-014

[DMTN-107], Graham, M.L., Bellm, E.C., Slater, C.T., et al., 2020, Options for Alert Production in LSST Operations Year 1, URL https://dmtn-107.lsst.io/,
Vera C. Rubin Observatory Data Management Technical Note DMTN-107

[LDM-324], Kantor, J., 2016, Data Management Information Security Plan, URL https://ls.st/LDM-324,
Vera C. Rubin Observatory LDM-324

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

[RTN-082], O'Mullane, W., 2024, Pixel Zone system security plan, URL https://rtn-082.lsst.io/,
Vera C. Rubin Observatory Technical Note RTN-082

[DMTN-135], O'Mullane, W., Dubois, R., Butler, M., Lim, K.T., 2023, DM sizing model and cost plan for construction and operations., URL https://dmtn-135.lsst.io/,
Vera C. Rubin Observatory Data Management Technical Note DMTN-135

[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

[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

[LSE-63], Tyson, T., Team, D., Collaboration, S., 2017, LSST Data Quality Assurance Plan, URL https://lse-63.lsst.io/,
Vera C. Rubin Observatory LSE-63

B Acronyms and Glossary

C Glossary

Alert A packet of information for each source detected with signal-to-noise ratio > 5 in a difference image by Alert Production, containing measurement and characterization parameters based on the past 12 months of LSST observations plus small cutouts of the single-visit, template, and difference images, distributed via the internet.

arcsec arcsecond second of arc (unit of angle).

camera An imaging device mounted at a telescope focal plane, composed of optics, a shutter, a set of filters, and one or more sensors arranged in a focal plane array.

Center An entity managed by AURA that is responsible for execution of a federally funded project.

ComCam The commissioning camera is a single-raft, 9-CCD camera that will be installed in LSST during commissioning, before the final camera is ready..

Commissioning A two-year phase at the end of the Construction project during which a technical team a) integrates the various technical components of the three subsystems; b) shows their compliance with ICDs and system-level requirements as detailed in the LSST Observatory System Specifications document (OSS, LSE-30); and c) performs science verification to show compliance with the survey performance specifications as detailed in the LSST Science Requirements Document (SRD, LPM-17).

Construction The period during which LSST observatory facilities, components, hardware, and software are built, tested, integrated, and commissioned. Construction follows design and development and precedes operations. The LSST construction phase is funded through the NSF MREFC account.

CUI Controlled Unclassified Information.

Data Release The approximately annual reprocessing of all LSST data, and the installation of the resulting data products in the LSST Data Access Centers, which marks the start of the two-year proprietary period.

deg degree; unit of angle.

Department of Energy cabinet department of the United States federal government; the DOE has assumed technical and financial responsibility for providing the LSST camera. The DOE's responsibilities are executed by a collaboration led by SLAC National Accelerator Laboratory.

DOE Department of Energy.

GEO Geosynchronous Earth Orbit.

Incident An undesired event, which under slightly different circumstances, could have resulted in harm to people, damage to property, or loss to process.

IPsec Internet Protocol Security.

IT Information Technology.

LSE LSST Systems Engineering (Document Handle).

LSST Legacy Survey of Space and Time (formerly Large Synoptic Survey Telescope).

monitoring In DM QA, this refers to the process of collecting, storing, aggregating and visualizing metrics.

MPC Minor Planet Center.

NAT Network Address Translation.

National Science Foundation primary federal agency supporting research in all fields of fun-

damental science and engineering; NSF selects and funds projects through competitive, merit-based review.

NIST National Institute of Standards and Technology (USA).

NSF National Science Foundation.

OOB Out Of Bound (Alternative network access).

Operations The 10-year period following construction and commissioning during which the LSST Observatory conducts its survey.

OSS Observatory System Specifications; LSE-30.

patch An quadrilateral sub-region of a sky tract, with a size in pixels chosen to fit easily into memory on desktop computers.

postage stamp Image cutouts that are 30x30 arcseconds, centered on an Object, and included in every Alert.

RSP Rubin Science Platform.

Science Platform A set of integrated web applications and services deployed at the LSST Data Access Centers (DACs) through which the scientific community will access, visualize, and perform next-to-the-data analysis of the LSST data products.

SLAC SLAC National Accelerator Laboratory.

SLAC National Accelerator Laboratory A national laboratory funded by the US Department of Energy (DOE); SLAC leads a consortium of DOE laboratories that has assumed responsibility for providing the LSST camera. Although the Camera project manages its own schedule and budget, including contingency, the Camera team's schedule and requirements are integrated with the larger Project. The camera effort is accountable to the LSSTPO..

SOC Security Operations Centre.

software The programs and other operating information used by a computer..

SSD Solid-State Disk.

Summit The site on the Cerro Pachón, Chile mountaintop where the LSST observatory, support facilities, and infrastructure will be built.

Systems Engineering an interdisciplinary field of engineering that focuses on how to design and manage complex engineering systems over their life cycles. Issues such as requirements engineering, reliability, logistics, coordination of different teams, testing and evaluation, maintainability and many other disciplines necessary for successful system development, design, implementation, and ultimate decommission become more difficult when dealing with large or complex projects. Systems engineering deals with work-processes, optimization methods, and risk management tools in such projects. It overlaps technical and human-centered disciplines such as indus-

trial engineering, control engineering, software engineering, organizational studies, and project management. Systems engineering ensures that all likely aspects of a project or system are considered, and integrated into a whole.

TLS Transport Layer Security.

USDF United States Data Facility.

Validation A process of confirming that the delivered system will provide its desired functionality; overall, a validation process includes the evaluation, integration, and test activities carried out at the system level to ensure that the final developed system satisfies the intent and performance of that system in operations.

VPN virtual private network.