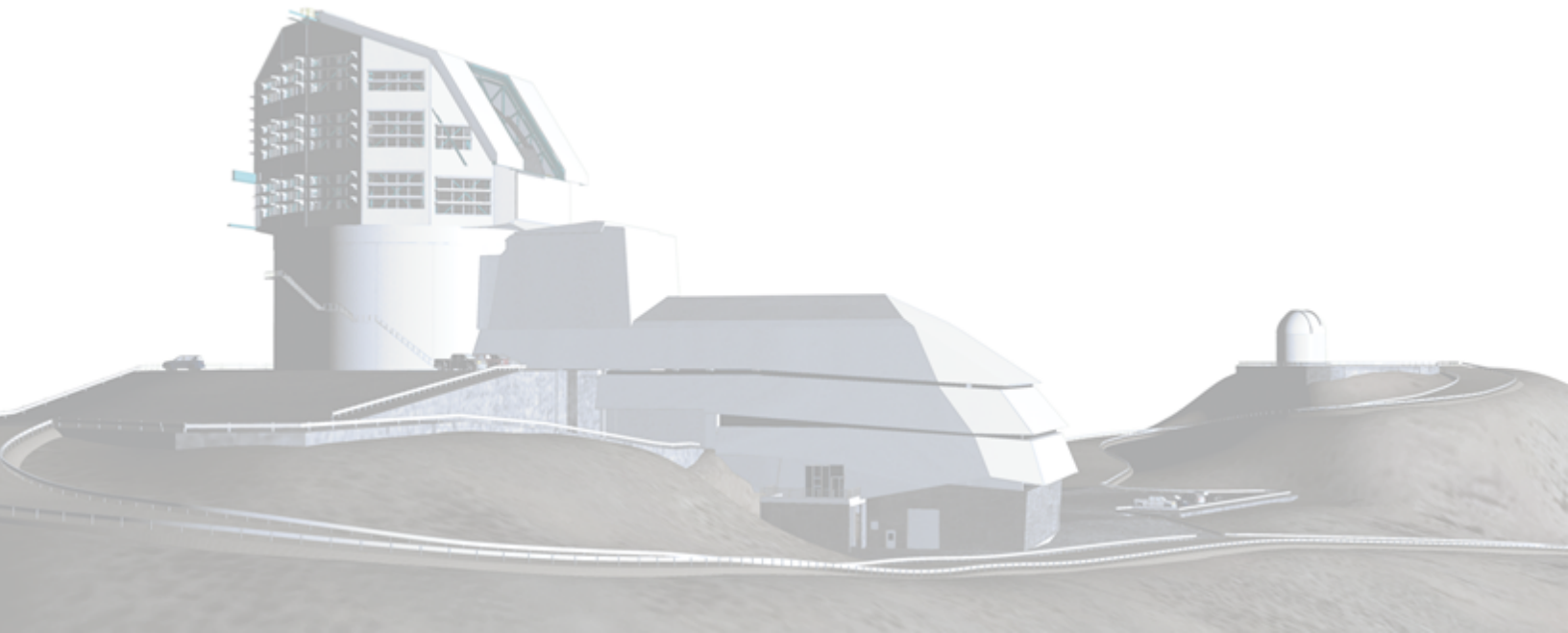

Vera C. Rubin Observatory
Data Management

CUI Rubin Observatory Data Security Standards Response

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

DMTN-199

Latest Revision: 2021-07-26

Abstract

This is a response to the Controlled Unclassified Information (CUI) document from the agencies.

Change Record

Version	Date	Description	Owner name
0.1	2021-07-19	Unreleased. Set up structure	William O'Mullane

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

Contents

CUI Rubin Observatory Data Security Standards Response

1 Introduction

The agencies have provided a set of requirements for security which we asses here and provide initial cost impact analysis for.

The summary requirements (from the start of the document) are :

1. Encrypt data using strong, approved encryption standard, following NIST 800-171 standard for CUI at non-federal organizations.
2. Install firewalls to prevent unauthorized network access, guided by NIST 800-171 standard for CUI at non-federal organizations.
3. Delay public release of focal plane scientific data for at least 80 hours following the observation, with Alert Vetting System allowed to withhold up to 4 images per month for up to 10 days with need only for notification to be given to NSF/DOE. Delay public release of engineering and commissioning imaging data for at least 30 days.
4. Eliminate artificial Earth-orbiting satellites from prompt alerts by (a) automatically alerting only on streaks corresponding to motions slower than 30 deg/day relative to sidereal tracking, and (b) alerting on longer (faster) streaks only after the Alert Vetting System has determined that the streak does not correspond to an artificial satellite.
5. Perform Earth-orbiting satellite processing in a separate facility operated by a “trusted broker” that has access to appropriate satellite catalogs.
6. Publish nominal collection schedules for regular sky survey 24 hours in advance.
7. Request and receive advance approval of large sky regions for use without sidereal tracking prior to initial on-sky test observations; then, approved regions (for use without sidereal tracking) will be supplied to the Rubin Observatory operations team in advance of their use.

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

2 Cost Summary

Costs are detailed in each section below Table 1 gives a summary.

Table 1: This table provides an overview of all the costs associated with this change.

Item	Cost	Operations Cost
Encryption (Table 2)	$3,204,000	$3,204,000
Firewalls and physical security (Table 3)	$25,894	
Delayed Data Store	$800,000	$800,000
Alert Vetting		$16,330,000
Total Construction	**$4,029,894**	
Total Operations Cost		**$20,334,000**

3 Response to the requirements

There is an implication that we should follow NIST.SP.800-171, as for any standard that is open to some interpretation. We will have to show how we comply to the standard. This may take the form of a compliance matrix as shown in Appendix A. In this matrix and in this document we assume CUI refers to embargoed images before release to the collaboration. Hence it applies to Prompt Processing, the embargoed data store(s) and the summit in Chile. It does snot apply to DACs nor the actual alert stream.

We note SLAC should comply with NIST.FIPS.200, FIPS.99, 800-53 and 800-60 as a Federal agency. We assume our NIST 800-171 will also apply to SLAC since NIST 800-171 is derived from exactly these documents.

From Section 2.1 of NIST.SP.800-171 we note the 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 **?** we propose to buy four routers which can perform AES IPSec 256 bit encryption between Chile and SLAC. We will not transfer embargoed images to France - hence we should keep an secure data store at Chile and at SLAC for redundancy. Cost here is base on a quotation from Cisco as one of the vendors explicitly specified in the agency document.

See Table 2 for the cost breakdown.

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

Item	Cost	number	Total
Cisco Router	$800,000	$4	$3,200,000
Cabling	$1,000	$4	$4,000
Misc			
Total			**$3,204,000**
1 Refresh in Operations			$3,204,000

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 plan:

- 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.

We will do as requested and cost estimates are provided in Table 3.

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 tends to extend the project baseline.

I am not sure how to cost signage and labeling as required in NIST 171 3.8.4 [2]

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
Locks SLAC	$13	30	$390
Cameras Detectors SLAC	$2,000	1	$2,000
Sensors SLAC	$38	30	$1,140
Sensor hub SLAC	$448	1	$448
Locks Chile	$13	20	$260
Cameras Detectors Chile	$2,000	2	$4,000
Sensors Chile	$38	20	$760
Sensor hub Chile	$448	2	$896
Faster CPU to handle disk encryption on summit			$0
Labor to redeploy all summit systems	$100	160	$16,000
Labelling and signage (CUI)	$2,000	1	$2,000
Total			**$25,894**

3.3 Delay public release

The best approach here 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 [3]. 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 a 30 day store for Full images and engineering data looking at DMTN-135 table table 40 this comes out to about 500TB of usable disk. Table 4 gives the cost calculation or this.

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	**$800,000**	
Ops Cost at least 1 Refresh	$800,000	

[2] https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf
[3] https://min.io/product/enterprise-object-storage-encryption

3.4 Eliminate earth orbiting satellites

Rubin does not publish alerts for streaks. A subset of streaks, potentially consistent with Earth-orbiting satellites or Solar System objects, will be evaluated by the AVS. AVS is under discussion currently in terms of design and how it may be implemented. The cost here is mainly FTE related the current OPS plan contains 2.5 FTE for this work. There is an unknown hardware aspect here - assuming a database already exists a fast front end server will still be needed with some redundancy. The cost of delaying the data in an encrypted store is already covered in Section 3.3 An estimate is given in Table 5.

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

Description	Cost	Count	Total
FTE per year	$500,000.00	2.5	$1,250,000
Mission years		10	$12,500,000
Pre operations years		3	$3,750,000
Front end server	$20,000.00	2	$40,000
1 server refresh			$40,000
Total			**$16,330,000**

3.5 Perform earth orbiting satellite processing in separate facility

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

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 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 prropcedurally and as such will not produce a delta cost on the project.

4 Conclusion

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
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
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	Cristian Richard - does this include SUDO ? Does this mean POSIX auditing?
3.1.8 Limit unsuccessful login attempts.	N	Y	I don't believe we do this now but we can; this is not done for ssh on hosts or network equipment. Web Services such as love, foreman, ipa console, nublado, etc. may need rate limiting
3.1.9 Provide privacy and security notices consistent with applicable CUI rules.	N	Y	Check login notices etc.
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	Cristian - not sure if we do this now ..
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	CUI 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 controllimit 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.
3.1.21 Limit use of portable storage devices on external systems.	N	Y	CristianRichard - impliesn no USB drives etc enabled ...
3.1.22 Control CUI posted or processed on publicly accessible systems.	Y	Y	We do not intend to post CUI 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.
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 implment SUDO lists to restrict access.
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	I think 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	Not sure we do this now - Cristian Richard ..
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 andor 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.		Y	Cristian .. Richard
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.govfilescui20161206-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	Cristian Richard
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.			
3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.			
3.10 PHYSICAL PROTECTION			
3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.			
3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.			
3.10.3 Escort visitors and monitor visitor activity.			
3.10.4 Maintain audit logs of physical access.			
3.10.5 Control and manage physical access devices.			
3.10.6 Enforce safeguarding measures for CUI at alternate work sites.			
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.			
3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.			
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.			
3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.			
3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.			
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.28			
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.			
3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.			
3.13.3 Separate user functionality from system management functionality.			
3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.			
3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.			
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).			
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).			

3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.			
3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.			
3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.			
3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.			
3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29			
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.			
3.13.15 Protect the authenticity of communications sessions.			
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.	N	N	
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		**79**	
Total Rubin Complies with in 2021		**51**	

B References

[DMTN-135], Butler, M., Lim, K.T., O'Mullane, W., 2019, *DM sizing model and purchase plan for the remainder of construction.*, DMTN-135, URL http://DMTN-135.lsst.io

[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

[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

C Acronyms

Acronym	Description
AES	Advanced Encryption Standard
CUI	Controlled Unclassified Information
DM	Data Management
DMTN	DM Technical Note
DOE	Department of Energy
IP	Internet Protocol
NIST	National Institute of Standards and Technology (USA)
NSF	National Science Foundation
SLAC	SLAC National Accelerator Laboratory
VPN	virtual private network
deg	degree; unit of angle