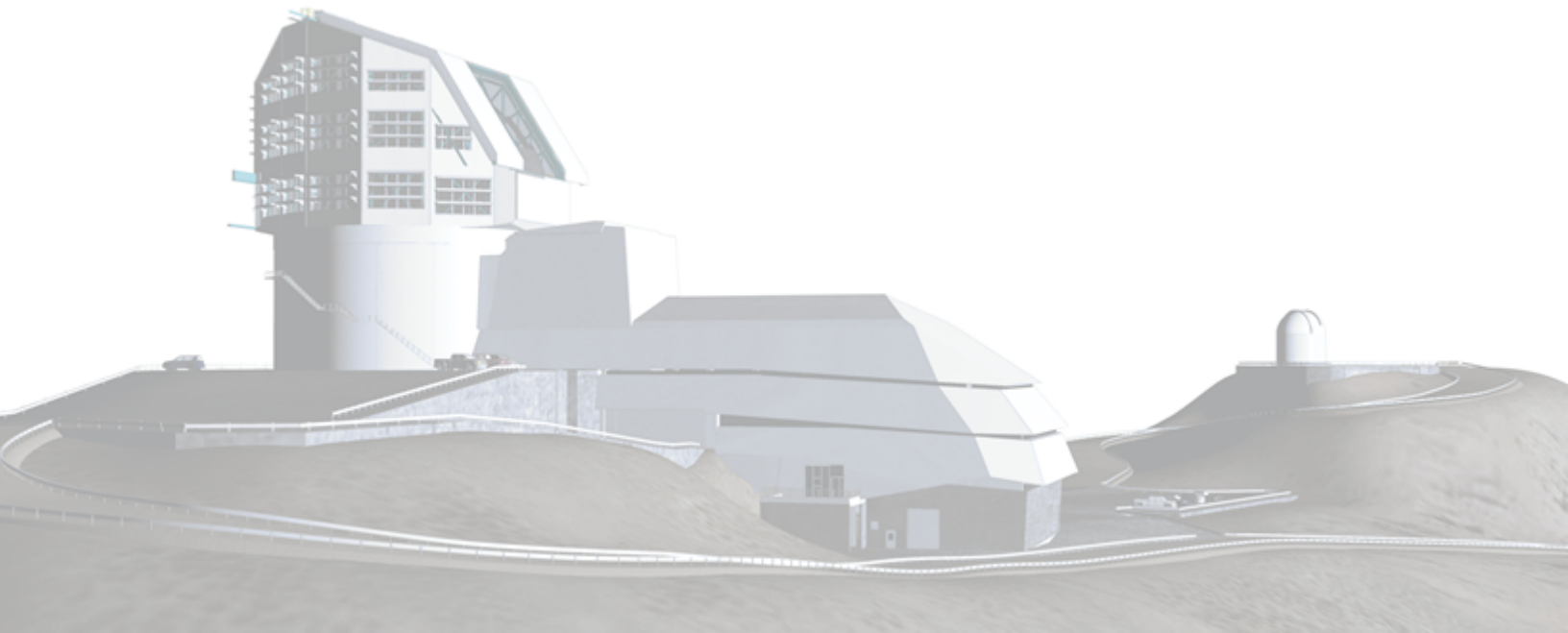
Vera C. Rubin Observatory
Data Management

CUI Rubin Observatory Data Security Standards Response

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

DMTN-199

Latest Revision: 2021-07-20



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

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.

We assume this applies to CUI, which we interpret as the embargoed image data 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].

3.1 Encrypt Data

3.2 Install Firewalls

3.3 Delay public release

3.4 Eliminate earth orbiting satellites

3.5 Perform earth orbiting satellite processing in separate facility

3.6 Publish nominal schedule

[1] {confidentiality, availability,integrity}

3.7 Request approval for non sidereal tracking

4 Conclusion

A Compliance with NIST Standard

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

NIST 800-171	2021 Status	Intended Compliance
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.	Y	Y
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.	Y	Y
3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.	Y	Y
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
3.1.8 Limit unsuccessful logon attempts.	N	Y
3.1.9 Provide privacy and security notices consistent with applicable CUI rules.	N	Y
3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	Y	Y
3.1.11 Terminate (automatically) a user session after a defined condition.	Y	Y
3.1.12 Monitor and control remote access sessions.		Y
3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Y	Y
3.1.14 Route remote access via managed access control points.	Y	Y
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
3.1.17 Protect wireless access using authentication and encryption.	Y	Y
3.1.18 Control connection of mobile devices.	Y	Y
3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23	Y	Y
3.1.20 Verify and controllimit connections to and use of external systems.	Y	Y
3.1.21 Limit use of portable storage devices on external systems.	N	Y
3.1.22 Control CUI posted or processed on publicly accessible systems.	Y	Y
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.		
3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.		
3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.		
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.		

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.		
3.3.3 Review and update logged events.		
3.3.4 Alert in the event of an audit logging process failure.		
3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.		
3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.		
3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.		
3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.		
3.3.9 Limit management of audit logging functionality to a subset of privileged users.		
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.		
3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.		
3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.		
3.4.4 Analyze the security impact of changes prior to implementation.		
3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.		
3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.		
3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.		
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.		
3.4.9 Control and monitor user-installed software.		
3.5 IDENTIFICATION AND AUTHENTICATION		
3.5.1 Identify system users, processes acting on behalf of users, and devices.		
Common device identifiers include Media Access Control (MAC), Internet Protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring identification may be defined by type, by device, or by a combination of typedevice.		
3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.		
3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.24 25		
3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non- privileged accounts.		
3.5.5 Prevent reuse of identifiers for a defined period.		
3.5.6 Disable identifiers after a defined period of inactivity.		
3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.		
3.5.8 Prohibit password reuse for a specified number of generations.		
3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.		

3.5.10 Store and transmit only cryptographically-protected passwords.		
3.5.11 Obscure feedback of authentication information.		
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.		
3.6.2 Track, document, and report incidents to designated officials andor authorities both internal and external to the organization.		
3.6.3 Test the organizational incident response capability.		
3.7 MAINTENANCE		
3.7.1 Perform maintenance on organizational systems.26		
3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.		
3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.		
3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.		
3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.		
3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.		
3.8 MEDIA PROTECTION		
3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.		
3.8.2 Limit access to CUI on system media to authorized users.		
3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.		
3.8.4 Mark media with necessary CUI markings and distribution limitations.27		
3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.		
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.		
3.8.7 Control the use of removable media on system components.		
3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.		
3.8.9 Protect the confidentiality of backup CUI at storage locations.		
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
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.		
3.14 SYSTEM AND INFORMATION INTEGRITY		
3.14.1 Identify, report, and correct system flaws in a timely manner.		
3.14.2 Provide protection from malicious code at designated locations within organizational systems.		
3.14.3 Monitor system security alerts and advisories and take action in response.		
3.14.4 Update malicious code protection mechanisms when new releases are available.		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
3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.		Y
Total requirements		**109**
Total Rubin lintends to comply with		**26**

Total Rubin Complies with in 2021		**17**

B References

[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
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
deg	degree; unit of angle