

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

1	Introduction	1
2	Cost Summary	2
3	Response to the requirements	2
	3.1 Encrypt Data	3
	3.2 Install Firewalls and other physical security devices	3
	3.3 Delay public release	4
	3.4 Eliminate earth orbiting satellites	5
	3.5 Perform earth orbiting satellite processing in separate facility	5
	3.6 Publish nominal schedule	5
	3.7 Request approval for non sidereal tracking	6
4	Conclusion	6
Α	Compliance with NIST Standard	6
В	References	9
C	Acronyms	10



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 (Table 4)	\$800,000	\$800,000
Alert Vetting System (Table 5)		\$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

NIST 1.7.1 Section 3.10.6 pulls in extra standards for remote work namely ? and ?. ? 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 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. Since these documents were written as guidance we will take note of them but may not always follow all recommendations in all cases.

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 encryp-			\$0
tion on summit			
Labor to redeploy all summit sys-	\$100	160	\$16,000
tems			
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	

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

³https://min.io/product/enterprise-object-storage-encryption



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	

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 Compli- ance	Note
3.1 ACCESS CONTROL			
3.1.1 Limit system access to authorized users, processes acting on behalf of autho-	Υ	Y	
rized users, and devices (including other systems).			
3.1.2 Limit system access to the types of transactions and functions that authorized	N	Y	There are many non-administrative users with unrestricted sudo ac-
users are permitted to execute.			cess
3.1.3 Control the flow of CUI in accordance with approved authorizations.	Υ	Y	
3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity with-	N	Y	Principle of least privilege is applied. Many users have access to
out collusion.			hosts that is unneeded.
3.1.5 Employ the principle of least privilege, including for specific security functions	N	Y	Targeted sudo rules are needed for common operations
and privileged accounts.			
3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.	Υ	Y	
3.1.7 Prevent non-privileged users from executing privileged functions and capture		Y	Cristian Richard - does this include SUDO ? Does this mean POSIX
the execution of such functions in audit logs.			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	Υ	Y	This is our policy.
data after a period of inactivity.			
3.1.11 Terminate (automatically) a user session after a defined condition.	N	Y	ssh sessions are generally not limited on hosts; some network equip-
			ment has timeouts set; nublado has a session limit for notebooks?
3.1.12 Monitor and control remote access sessions.	N	Υ	Cristian - not sure if we do this now
3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Υ	Y	VPN is in use
3.1.14 Route remote access via managed access control points.	N	Υ	Bastion nodes – LHN is an open back door with no ACLs
3.1.15 Authorize remote execution of privileged commands and remote access to	Υ	Y	
security-relevant information.			
3.1.16 Authorize wireless access prior to allowing such connections.	Υ	Υ	All devics attaching in Chile need to be registered by Mac address.
3.1.17 Protect wireless access using authentication and encryption.	Υ	Υ	
3.1.18 Control connection of mobile devices.	Υ	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	Υ	Y	CUI will not exist on mobile devices - in the case where an image may
5 5 Energy Co. 5.1 mobile devices and mobile comparing platforms.25	'	'	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.	Υ	Y	This implies vetting of devices that connect to the control network
	1	'	- 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	<u> </u>		



terms are made aware of the excurity risks avocational with their activative and of the applicable policitors, standards, and precisive related to the security of those spectroms. 2.2.2 France shut, personnel are trained to carry out their assigned information 3.2.3 France shut, personnel are trained to carry out their assigned information 3.2.3 France shut, personnel are trained to carry out their assigned information 3.3.3 France and terms system and to grant protection of the electric received to enable of the motioning, analysis, investigation, and reporting of unlineador unaudorized systems. 3.3.4 France that the extense of insolution glant plants are care to unaudorized systems. 3.3.4 France that the extense of insolution glants are care to unaudorized systems. 3.3.4 France that the event of an audit logging process failure. 3.3.4 France that the event of an audit logging process failure. 3.3.5 France and terrorizedwa, analysis, and reporting processes for investigation, and reporting process failure. 3.3.6 France and recording and accountable for their actions. 4. Y 4. We may look for a third party centract for this. 3.3.4 France that the event of an audit logging process failure. 5. Y 4. Y 4. We may look for a third party centract for this. 3.3.4 France that the event of an audit logging process failure. 7. Y 8. Y 8. Y 8. Y 9. Y 9. We may look for a third party centract for this. 9. Y 9. Y 9. We may look for a third party centract for this. 9. Y 9. Y 9. We may look for a third party centract for this. 9. Y 9. Y 9. We may look for a third party centract for this. 9. Y 9. Y 9. Y 9. We may look for a third party centract for this. 9. Y 9. Y 9. Y 9. We may look for a third party centract for this. 9. Y 9. Y 9. Y 9. Y 9. We may look for a third party centract for this. 9. Y 9. Y 9. We may look for a third party centract for this. 9. Y 9. Y 9. We may look for third party centract for this. 9. Y 9. Y 9. We may look for third party centract for this. 9. Y	3.2.1 Ensure that managers, systems administrators, and users of organizational sys-	Υ	Υ	
applicable policies, standards, and procedures related to the security of those systems. 3.2.3 Frozen that personnel are trained to carry out their oxiggred information security-related dudes and responsibilities. 3.2.3 Frozen security awareness training an executing and reporting potential in V V We would like to do more here like capture flag exercises for developeds. 3.2.3 Frozen security awareness training an executing and reporting potential in V V We would like to do more here like capture flag exercises for developeds. 3.2.3 Frozen and posity, investigation, and propring of curiosate or unauthorized or propring for the propring of curiosate or v V V V V V V V V V V V V V V V V V V				
sems. 3.2.2 Finuse that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Finuse security assertions around a record of the control of	•			
security related durines and responsibilities. 2.3.2 Provide script waveness starling on recognizing and reporting potential in the control of insider threat. 3.3.1 Crates and retain system sudd logs and records to the extent needed to enable the control of recognizing and starling of the control of the				
3.3 AUDIT AND ACCOUNTABLE TO THE CONTROL OF THE CON	3.2.2 Ensure that personnel are trained to carry out their assigned information	N	Υ	
3.3 AUDIT AND ACCOUNTABLE TO THE CONTROL OF THE CON	security-related duties and responsibilities.			
Jackson or director threat. 3.3.1 Critare from ferain system audit logs and records to the extern needed to enable of the homenturing, analysis, investigation, and records to the extern needed to enable of the homenturing, analysis, investigation, and records to the extern needed to enable of the homenturing, analysis, investigation, and records to the external needed to enable of the homenturing, analysis, investigation, and records the following of the actions. 7. V. V. We may look for a third party contract for this. 3.3.3 Florent his the actions of individual system users can be uniquely traced to v. V. V. We may look for a third party contract for this. 3.3.4 Albert in the rever of an audit ligging process failure. 8.3.5 Foreities audit record relation, analysis, and reporting processes for investigation and response to indications of uniawally unatharbriesd, supplicit, or unusual activity. 8.3.6 Foreide audit record relation, and and report generation to support on demand of anylogism of reporting. 8.3.7 Foreide audit record relation and audit logging process failure. 8.3.8 Foreide audit record relation and audit logging process and synchronizes internal system. 8.3.9 Foreide audit information and audit logging process and synchronizes internal system. 8.3.1 Foreide audit information and audit logging process and synchronizes internal system. 8.3.2 Foreide audit information and audit logging process and synchronizes internal system. 8.3.3 Foreide audit information and audit logging process failure. 8.3.4 Foreida and relationship for information and audit logging process and process. 9. V. V. We have CCBs and code change process in place which also cover the late of inspiratementurin. 9. V. V. We have CCBs an	3.2.3 Provide security awareness training on recognizing and reporting potential in-	Υ	Y	We would like to do more here like capture flag exercises for devel-
3.3.4 Crose and recard system and list logs and records to the extent needed to enable the monotroning, analysis, investigation, and reporting for Individual system users can be uniquely traced to visible actions of individual system users can be uniquely traced to visible actions of individual system users can be uniquely traced to visible actions of individual system users can be uniquely traced to visible actions of individual system users can be uniquely traced to visible actions of individual system users can be uniquely traced to visible actions of individual system users can be uniquely traced to visible actions of individual system users can be uniquely traced to visible actions of individual system users can be uniquely traced to visible actions of individual system of the control of the visible actions of individual system of the control of the visible actions of individual system of the control of the visible action of individual system of the visible actions of individual system of the visible action of individual systems of the visible action of individual s				
3.3.1 critical and retain system audit logs and records to the extent needed by the monitoring analysis, investigation of reporting of inherity of the actions. 3.2.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.4 Environment of the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.4 Environment of the actions of the actions. 3.3.5 Environment of the actions of the actions. 3.3.6 Environment of the actions				1,000
the monitoring, analysis, investigation, and reporting of unlowful or unauthorized yes term activity. 3.3.2 Resure that the actions of incividuals system users can be uniquely traced to 3.3.3 Review and update logged events. 3.3.3 Review and update logged events. 3.3.3 Review and update logged events. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation. 3.3.6 A Aller in the redictions of univalivity unauthorized, supposition, or unautial activity. 3.3.6 Provide audit record reduction and reporting processes for investigation. 3.3.6 Provide audit record reduction and reporting processes for investigation. 3.3.6 Provide audit record reduction and reporting processes for investigation. 3.3.6 Provide audit record reduction and report generation to support on-demand and response generate intensionally for audit records. 3.3.8 Provide audit record reduction and report generation to support on-demand and response generate intensionally for audit logging functionally to a subset of privileged users. 4. CONSCRIBATION MANAGEMENT 3.4. Establish and enforce security configurations and inventories of organizational by systems (including hardware, software, firmware, and documentation throughout the respective system development life cycles. 3.4. Establish and enforce security configurations estings for information technology products employed in organizational systems. 3.4. Foreign and an animal management of support and interesting in information technology and animal management of supports and interesting interesti		٧	V	
tem activity. 3.3.2 First that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.2 First first event of an audit logging process failure. 3.3.4 First in the event of an audit logging process failure. 3.3.5 Foreign active record reduction of unlawful, unauthorized, suspicious, or unusual activity. 3.3.5 Foreign active record reduction and report generation to support on-definition of unlawful, unauthorized, suspicious, or unusual activity. 3.3.5 Foreign active record reduction and report generation to support on-definition of unlawful, unauthorized, suspicious, or unusual activity. 3.3.5 Foreign active record reduction and report generation to support on-definition and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.5 Foreign active record reduction and report generation to support on-definition and report generation of unlawful, unauthorized, suspicious, or unusual activity. 3.3.5 Foreign active record reduction and report generation to support on-definition and report generation of support on-definition and reporting. 3.3.5 Foreign active record reduction and surface foreign active active and surface foreign active acti		•	'	
3.3.2 Review and updates logged events. 3.3.3 Never in the vent of an audit ologging process failure. 9.				
shose users, so they can be held accountable for their actions. 3.3.4 Retri in the event of an audit logging process failure. 8.7. Y V We may look for a third party contract for this. 8.8. A V Again shall look for third party contract for this. 8.9. A V Again shall look for third party contract for this. 8.9. A V Again shall look for third party contract for this. 8.9. A V Again shall look for third party contract for this. 8.9. A V Again shall look for third party contract for this. 8.9. A V Again shall look for third party contract for this. 8.9. A V V Again shall look for third party contract for this. 8.9. A V V V V V V V V V V V V V V V V V V		V		
3.3.3 Alert in the rewnt of an utilit logging process failure. N Y Y Again shall look for third party contract for this. 3.3.4 Peri that rewnt of an utilit party contract for this. 3.3.5 Provide audit record relews, analysis, and reporting processes for investigation and response to indications of unably unauthorized support on-demand analysis and reporting. 3.3.6 Provide a system capability that compares and synchronizes internal system (onclose with an authorizative source to generate timestamps for audit record reduction and report and surface to generate timestamps for audit record reduction and report and surface to generate timestamps for audit record. 3.3.7 Provide a system capability that compares and synchronizes internal system (onclose with an authorizative source to generate timestamps for audit record reduction and report and utility to a subset of privileged users. 3.3.8 Provide a system development life cystem. 3.4.1 Combinishment of audit logging functionality to a subset of privileged users. 3.4.2 Fastbasin and minitaria baseline configurations settings for information technology period in the security impact of changes prior to implementation. 3.4.3 Fastbasin and enforce captivity configuration settings for information technology associated with changes to organizational systems. 3.4.4 Fastbasin changes to organizational systems. 3.4.5 Postpas, comment, approve, and olegaptove, and logical access restrictions y associated with changes to organizational systems. 3.4.5 Postpas, comment, approve, and olegaptove, and logical access restrictions of the provide only essential capabilities. 3.4.5 Postpas, comment, approve, and olegaptove, and logical access restrictions of the provide only essential capabilities. 3.5.4 Provides adult of the provides o			'	
3.3.4 First in the event of an audit logging process failure. 3.5.6 Certable subtrict record review maybe, and reporting processes for investigation and response to indications of unlawful, unauthorited, suspicious, or unusual activity. 3.6 Frovide audit record review and an export generation to support on-demand an analysis and reporting. 3.7 Frovide a system capability that compares and synchronizes internal system (analysis and reporting.) 3.8 Frovide audit forgrantion and and togging functionality to a subset of privileged users. 3.8 Frovide audit information and audit logging functionality to a subset of privileged users. 3.4 CORHGURATION MANAGEMENT 3.4.1 Establish and enforce security configurations and inventories of organizational systems (including hardware, software, furnware, and documentation) throughout the respective system development life (cycles.) 3.4.2 Establish and enforce security configuration settings for information technology or products employed in organizational systems. 3.4.3 Franck, review, approve or disapprove, and log changes to organizational systems. 3.4.3 Franck, review, approve or disapprove, and log changes to organizational systems. 3.4.3 Franck, review, approve or disapprove, and log changes to organizational systems. 3.4.3 Franck, review, approve or disapprove, and log changes to organizational systems. 3.4.3 Franck, review, approve or disapprove, and log changes to organizational systems. 3.4.3 Franck, review, approve or disapprove, and log changes to organizational systems. 3.4.3 Franck, review, approve or disapprove, and log changes to organizational systems. 3.4.3 Franck, review, approve or disapprove, and log changes to organizational systems. 3.4.3 Franck, review, approve or disapprove, and log changes to organizational systems. 4.4.5 Employer the development in the control of programs, functions, ports, y 4.5.5 Employer procedular through the control of programs, functions, ports, y 5.5.6 Employer procedular through the control of programs, funct		D	- V	We may look for a third party contract for this
3.3.5 Provide audit record releveus analysis, and reporting processes for investigation and response to indications of unlawful unautantrices, assignations, or unsual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and report generation 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 timestamps for audit record. 3.3.8 Protect audit information and audit logging functionality to a subset of privileged users. 3.3.8 Protect audit information and audit logging functionality to a subset of privileged users. 3.4.1 CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations settings for information technology products employed in organizational systems. 3.4.2 Establish and maintain baseline configurations estings for information technology products employed in organizational systems. 3.4.3 Track, reway approve or disengiture and analysis of the security impact of changes prior to implementation. 3.4.3 Track, reway approve or disengiture and enforce physical and logical access restrictions by a second continuous process. 3.4.4 Analyze the security impact of changes prior to implementation. 3.5.4 Problem, document, approve, and enforce physical and logical access restrictions provided only the security impact of changes to organizational systems. 3.4.4 Problem, document, approve, and enforce physical and logical access restrictions or provide only experiture and programs, functions, ports, viving and programs, f				We may look for a third party contract for this.
and response to indications of unlawful, unauthorized, susplicitus, or unusual activity, 3.3 Fronzie auth record reduction and report generate into support or or-demand analysis and reporting. 3.3 Provide a system capability that compares and synchronizes internal system of clocks with an authoritative source to generate timestamps for audit records. 3.3 Provide audit information and audit foliging floor form unauthorized access, or modification, and deletion. 3.4 Constrained and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development file cycles. 3.4.2 Establish and enforce security configuration settings for information technology or products employed in organizational systems. 3.4.3 Franky, review, approve or disapprove, and log changes to organizational systems. 3.4.4 Establish and enforce security configuration settings for information technology or products employed in organizational systems. 3.4.5 Define, document, approve, and enforce physical and logical ancess restrictions associated with changes to organizational systems. 3.4.6 Finelyby freprinciple class tructionality by configuring organizational systems to provide only essential capabilities. 3.4.7 Restrict, dashie, or prevent the use of nonessential programs, functions, ports, and approach of the provided of the provided organizational systems. 3.5 Julianity systems with the provided containers. 3.5 Julianity systems users, processes, or devices, as a previous of the provided and provided an	== =:			A series also III to all for a their all a series as a series at few their
3.3.7 Provide a upstem coabelity that compares and synchronizes internal system (analysis and reporting). 3.3.7 Provide a system coabelity that compares and synchronizes internal system (analysis and reported). 3.3.8 Protect audit information and audit logging tools from unauthorized access, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4.1 CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventorics 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, reckine, approve, and enforce physical and logical access restrictions by tems. 3.4.4 Analyze the security impact of changes prior to implementation. 3.4.5 Employ the principle of least functionality by configuration settings for information settings for information technology products employed in organizational systems. 3.4.4 Farablish and enforce security configurations restrictions by 3.4.5 Employed the security impact of changes prior to implementation. 3.4.5 Employed the security impact of changes prior to implementation. 3.4.5 Employed the security impact of changes prior to implementation. 3.4.6 Employed the security impact of changes prior to implementation. 3.4.6 Employed the security impact of changes prior to implementation. 3.4.6 Employed the security impact of changes prior to implementation. 3.4.7 Restrict, disable, or prevent the use of inauthorized software or denytal permit-by-exception (blackisting) policy to allow the execution of authorized software. 3.4.8 Apply denyt-by-exception (blackisting) policy to provide and permit of the security of the identities of the security of the identities of the security of the identities of the security		N	Y	Again shall look for third party contract for this
Janabysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system (diocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4.0 CARRIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, furnware, and documentation) throughout the respective system development if cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Farak, review, approve or disapprove, and elogical access restrictions as a system of the security impact of changes prior to implementation. 3.4.5 Define, document, approve, and enforce physical and oligical access restrictions as a system continuation of the security of the security of last functionality by configuring organizational systems. 3.4.6 Employ the phrespital capabilities. 3.4.7 Reported, display the privacy of class functionality by configuring organizational systems by produce only exercise of last functionality by configuring organizational systems. 3.4.8 Apply temp-by-exception (blacklisting) policy to prevent the use of unauthorized software or darphy-by-exception (blacklisting) policy to prevent the execution of authorized software. 3.4.8 Capply temp-by-exception (blacklisting) policy to prevent the execution of authorized software. 3.4.9 Corticular monitor user-installed software. 3.5 Destriction and protection of the privileged account of the privileged accounts and for neutriness and authorities of a defined period. 3.5 Destricti			- V	
3.3.7 Provide a system capability that compares and synchronizes internal system (choics with an authoritative source generate timestarps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, in a confidation, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4.1 Establish and deletion. 3.4.2 Establish and maintain baseline configurations and inventories of organizational viewell baseline in systems (including hardware, software, firmware, and documentation) throughout the especies system development fle cycles. 3.4.2 Establish and enforce security configuration settings for information technology in control and enforce security configuration settings for information technology and the especies system development fle cycles. 3.4.3 Tank, review, approve or disapprove, and log changes to organizational systems. 3.4.3 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. 3.4.4 Entity by the principle of least functionality by configuring organizational systems. 3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. 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. 3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, and protocols, and services. 3.4.8 Apply deny by exception (blocklisting) policy to prevent the use of unauthorized software. 3.4.9 Determinently-yexception (blocklisting) policy to prevent the use of unauthorized software. 3.4.9 Determinently-yexception (blocklisting) policy to prevent the use of unauthorized software. 3.5.1 Determinently-yexception (blocklisting) policy to allow the execution of authorized software. 3.5.2 Authoritation and	1 - 1	N	Y	
docks with an authoritative source to generate timestamps for audit records. 3.8 Protect autit information and walf logging tools from unauthorized access, modification, and deletion. 3.4 Control 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 or products employed in organizational systems. 3.4.2 Establish and enforce security configuration settings for information technology or products employed in organizational systems. 3.4.3 Establish and enforce security configuration settings for information technology or products employed in organizational systems. 3.4.4 Enabler the security impact of changes prior to implementation. 3.4.5 Define, document, approve, and enforce physical and logical access restrictions or associated with changes to organizational systems. 3.4.6 Enabler the principle of least functionality by configuring organizational systems or provide only essential cipabilities. 3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, you will be principle of least functionality by configuring organizational systems or provide only essential cipabilities. 3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, you will be principle of least functionality by configuring organizational systems. 3.4.8 Exployed physical and entire the principle of least functionality by configuring organizational systems or deployed containers. 3.4.8 Exployed physical and programs, functions, ports, your will be provided organizational systems or deployed containers. 3.4.8 Exployed physical and programs, functions, ports, your will be provided and monitor or exployed physical and systems. 3.4.9 Exployed physical and programs, functions, ports, your provided physical and programs, functions, ports, your provided phys				
3.3.8 Protect audit Information and audit logging tools from unauthorized access. Y Y Y ACCONFIGURATION MANAGEMENT 3.4.1 Establish and relation in Sealing of Control and Operations and Inventories of organizational systems (Including hardware, Software, Ermaner, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configurations and inventories of organizational systems (Including hardware, Software, Ermaner, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology of the products employed in organizational systems. 3.4.3 Tark, review, approve or disapprove, and log changes to organizational systems. 3.4.3 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. 3.4.3 February (Entotionality by configuring organizational systems). 3.4.5 Employer inclined in the second organizational systems. 3.4.6 Employer inclined fields inclinedally by configuring organizational systems. N Y We get a lot of this by mainly containerizing the applications and having users work within deployed containers. N Y We get a lot of this by mainly containerizing the applications and having users work within deployed containers. N Y We need to impliment SUDO lists to restrict access. Y Y Y Restrict Control and monitor user-installed software. N Y Y Restrict Control and monitor user-installed software. N Y Y Restrict Control and monitor user-installed software. N Y Y Restrict Control and monitor user-installed software. N Y Y Restrict Control and monitor user-installed software. N Y Y Restrict Control and monitor user-installed software. N Y Y Restrict Control and monitor user-installed software. N Y Y Restrict Control and monitor user-installed software. N Y Y Restrict Control and monitor user-installed software. N Y Y Restrict Control and monitor user-installed software. N Y		Y	Y	
inodification, and deletion. 3.3.9 Limit management of audit lingging functionality to a subset of privileged users. Y 3.4. CRAINER and maintain baseline configurations and inventories of organizational yestems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. At 12 Establish and enforce security configurations and inventories of organizational yestems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. At 12 Establish and enforce security configurations and inventories of organizational systems. 3.4.2 Establish and enforce security configurations and inventories of organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to 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 Establish and enforce security impact of changes prior to implementation. 4.4 A realyze the security impact of changes prior to implementation. 5.4.4 A realyze the security impact of changes prior to implementation. 7.4 V 8.4.5 We have CCBs and code change process in place which also cover them. 8.4.5 A realyze the security impact of changes prior to implementation. 9.4 V 9.4 V 9.4 We have CCBs and code change process in place which also cover them. 9.4 V 9.4 V 9.4 V 9.4 We have CCBs and code change process in place which also cover them. 9.4 V 9.4 V 9.4 V 9.4 V 9.4 V 9.4 V 9.4 We have CCBs and code change process in place which also cover them. 9.4 V 9.4 We past a lot of this by mainly containerizing the applications and having users work within deployed containers. 9.4 V 9.4 V 9.4 V 9.4 V 9.4 V 9.4 V 9.5 V 9.4 V 9.4 V 9.5 V 9.4 V 9.5 V 9.4 V 9.5 V 9.5 V 9.7 V 9.7 V 9.8 V 9.9 V				
3.3.9 Limit management of audit logging functionality to a subset of privileged users. 4 Y Y 4 CONFIGERATION 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 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 Ranabyze the security impact of changes prior to implementation. 3.4.5 Define, courment, approve, and enforce physical and logical access restrictions. 3.4.6 Employ the principle of least functionality by configuring 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 nonescential programs, functions, ports, or provide only essential capabilities. 3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software. 5.4.9 Control and monitor user-installed software. 7 Y 8.5.1 Identify system users, processes acting on behalf of users, and devices. 8.5.2 Lathenticate (or verify) the identities of users, processes, or devices, as a preveguiste to allowing access to organizational systems. 3.5.3 Fernotre a maintenance of control and network access to privileged accounts and for network access to non-privileged accounts. 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged accounts. 3.5.5 Previous reuse of identifiers for a defined period. 8.7 Y 9.7 Y 9.8 Authenticate or verify the identities of users, processes acting on the changes of characters when new password see or estated. 9.8 System users processes ac	== =	Υ	Y	
3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, software, 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. 3.4.3 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 Establish and enforce security impact of changes prior to implementation. 4.4.7 Y 4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. 5.4.6 Establish and enforce security impact of changes prior to implementation. 7.7 Y 8.4.7 Y 8.4.4 Capture than a sprove, and enforce physical and logical access restrictions associated with changes to organizational systems. 8.4.4 Capture principle of least functionality by configuring organizational systems by provide only essential capabilities. 8.4.7 Y 8.4.7 Y 8.4.8 Establish and enforce security impact of changes prior to implementation. 8.5.4 Physical security impact of changes prior to implementation. 9.4 Y 9.5 We get a lot of this by mainly containering the applications and having users work within deployed containers. 9.4 Y 9.5 We get a lot of this by mainly containering the applications and having users work within deployed containers. 9.4 Y 9.5 We need to impliment SUDO lists to restrict access. 9.5 Jean of the definition of user-installed software. 9.5 Jean of the definition of user-installed software. 9.5 Jean of the definition of user-installed software. 9.7 Y 1.5 Indicates of user-installed software. 9.8 Y 9.9 V 9.9 V 9.9 V 9.9 V 9	·			
3.4.1 Establish and maintain baseline configurations and inventories of organizational yestems (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. 3.4.4 Analyze the security impact of changes prior to implementation. 3.4.5 Define, document, approve, and enforce physical and logical access restrictions or associated with changes to organizational systems. 3.4.6 Employ the principle of least functionality by configuring organizational systems. 3.4.6 Employ the principle of least functionality by configuring organizational systems in provide only essential capabilities. 3.4.7 Restrict, dashle, or prevent the use of nonessential programs, functions, ports, provide only essential capabilities. 3.4.8 Pappy derty-by-exception (blacklisting) policy to prevent the use of unauthorized software and monitor user-installed software. 3.4.9 Control and monitor user-installed software. 3.5 Ildentify system users, processes acting on behalf of users, and devices. 3.5.1 Identify system users, processes acting on behalf of users, and devices. 3.5.2 Enforce and monitor user-installed software. 3.5.3 Enforce and monitor user-installed software. 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged accounts and for network access to on-privileged accounts. 3.5.5 Premotre remover Access to on-privileged accounts. 3.5.6 Premotre remover Access to on-privileged accounts. 3.5.7 Enforce a minimum passwoord complexity and change of characters when new your password are rested. 3.5.8 Premotre results of a defined period. 3.5.9 Frenotre results of a defined period of inactivity. 4.7 Your password results of a specified number of generati	3.3.9 Limit management of audit logging functionality to a subset of privileged users.	Υ	Y	
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 y products employed in opanizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. 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 or provide only essential capabilities. 3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, or provide only essential capabilities. 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 or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. 3.5.1 DENTIFICATION AND AUTHENTICATION 3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a pre-requisite to allowing access to organizational systems. 3.5.3 Desmittator authentication for local and network access to privileged accounts and for network access to organizational systems. 3.5.3 Desmittator authentication for local and network access to privileged and non-privileged accounts. 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. 3.5.5 Disability densities of a specified number of generations. 3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created. 3.5.8 Prohibity password reuse for a specified number of generations. 4 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.	3.4 CONFIGURATION MANAGEMENT			
the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.2 Establish and enforce security configuration settings for information technology and a services. 3.4.3 Track, review, approve or disapprove, and log changes to 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. 4.5 Particle, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems to provide only essential capabilities. 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, to provide only essential capabilities. 3.4.8 Appl development file of this by mainly containerizing the applications and having users work within deployed containers. 4.8 Appl development of this by mainly containerizing the applications and having users work within deployed containers. 4.9 Control and monitor user-installed software. 4.9 V V We need to implement SUDO lists to restrict access. 4.9 V V We need to implement SUDO lists to restrict access. 4.9 V V V V V V V V V V V V V V V V V V V	3.4.1 Establish and maintain baseline configurations and inventories of organizational	Υ	Y	We use mainly infrastructure as code approaches so the software is
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. 3.4.5 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. 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. 3.5.1 DIENTIFICATION AND AUTHORITICATION 3.5.1 Identify system users, processes acting on behalf of users, and devices. 3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prequisite 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 organizational systems. 3.5.3 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. 3.5.5 Province a minimum password complexity and change of characters when new passwords are created. 3.5.6 Disable identifiers for a defined period. 3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created. 3.5.10 Isosable interfers after a defined period of inactivity. 4 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. 3.5.10 Isosable force feedback of authentication information. 4 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.	systems (including hardware, software, firmware, and documentation) throughout			well tracked. IT inventory all the hardware.
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, ports, and services. 3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or energy and provide only exsential expansibilities. 3.4.9 Control and monitor user-installed software. 3.5.1 DENTIFICATION AND AUTHENTICATION 3.5.1 DENTIFICATION AND AUTHENTICATION 3.5.1 User and access to organizational systems. 3.5.3 User unitation for local and network access to privileged accounts and for network access to organizational systems. 3.5.4 Curthenticate for verify it delentities of users, processes, or devices, as a prevenuities to allowing access to organizational systems. 3.5.5 Pervent reuse of identifiers for a defined period. 3.5.6 Disable identifiers after a defined period. 3.5.7 Disable identifiers after a defined period. 3.5.8 Provent reuse of identifiers for a defined period. 3.5.8 Prohibit password reuse for a specified number of generations. 3.5.9 Provent reuse of identifiers for a defined period. 3.5.9 Disable identifiers after a defined period of inactivity. 3.5.9 Disable identifiers after a defined period of inactivity. 3.5.9 Disable identifiers after a defined period of inactivity. 3.5.10 Disable identifiers after a defined period of inactivity. 3.5.10 Disable identifiers after a defined period of inactivity. 3.5.10 Disable identifiers after a defined period of inactivity. 3.5.10 Disable identifiers after a defined period of inactivity. 3.5.10 Disable identifiers after a defined period of inact	the respective system development life cycles.			
3.4.3 Form to demonstrate the use of nonesential programs, functions, ports, protocols, and services. 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 deep-ty-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. 3.5.1 Identify system users, processes acting on behalf of users, and devices. 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 mechanisms for network access to privileged accounts. 3.5.4 Employ replay-resistrat unthentication mechanisms for network access to privileged and non-privileged accounts. 3.5.5 Prevent reuse of identifiers for a defined period of inactivity. 3.5.7 Prohibit password reuse for a specified number of generations. Y Y STANDARD AUTHENTICATION and provide accounts. 3.5.9 Policy in the properties of a specified number of generations. Y Y STANDARD AUTHENTICATION and provide accounts. 3.5.1 Dentify serior and provide accounts. 3.5.2 Freyent reuse of identifiers for a defined period of inactivity. 3.5.5 Prevent reuse of identifiers for a defined period of inactivity. 3.5.7 Frohotic aminimum password complexity and change of characters when new passwords are created. 3.5.9 Allow promorary password use for system logons with an immediate change to a permanent password. Y Y AURA have insurance which covers this. But we really should have a contract to look over logs	3.4.2 Establish and enforce security configuration settings for information technology	Υ	Υ	
3.4.3 Form to demonstrate the use of nonesential programs, functions, ports, protocols, and services. 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 deep-ty-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. 3.5.1 Identify system users, processes acting on behalf of users, and devices. 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 mechanisms for network access to privileged accounts. 3.5.4 Employ replay-resistrat unthentication mechanisms for network access to privileged and non-privileged accounts. 3.5.5 Prevent reuse of identifiers for a defined period of inactivity. 3.5.7 Prohibit password reuse for a specified number of generations. Y Y STANDARD AUTHENTICATION and provide accounts. 3.5.9 Policy in the properties of a specified number of generations. Y Y STANDARD AUTHENTICATION and provide accounts. 3.5.1 Dentify serior and provide accounts. 3.5.2 Freyent reuse of identifiers for a defined period of inactivity. 3.5.5 Prevent reuse of identifiers for a defined period of inactivity. 3.5.7 Frohotic aminimum password complexity and change of characters when new passwords are created. 3.5.9 Allow promorary password use for system logons with an immediate change to a permanent password. Y Y AURA have insurance which covers this. But we really should have a contract to look over logs	, , ,			
the infrastructure as code. 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 denry-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. 3.5.1 Identify system users, processes acting on behalf of users, and devices. 3.5.3 Use multifactor authentication for local and network access to privileged and non-privileged accounts. 3.5.4 Employ replay-resistant authentication mechanisms for network access to 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 Prevent reuse of identifiers for a defined period. 3.5.8 Polibiti password reuse for a specified number of generations. 3.5.9 Allow temporary password use for system identifiers or generations on the intendition of protocome in a minediate change to permanent password. 3.5.10 Identifiers after a defined period of inactivity. 3.5.10 Identifiers password reuse for a specified number of generations. 4 Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y		Υ	Y	We have CCBs and code change process in place which also cover
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 deep-tyb-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. 3.5.1 Identify system users, processes acting on behalf of users, and devices. 3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prequalist to allowing access to organizational systems. 3.5.4 Employ replay-resistant authentication mechanisms for network access to non-privileged accounts. 3.5.5 Prevent reuse of identifiers for a defined period. 3.5.6 Process reuses of complexity and change of characters when new yasswords are created. 3.5.9 Allow terruses of identifiers for a specified number of generations. 4 Y Y Y Supermonent of the proposed of inactivity. 5.5.9 Forlow traves of identifiers for a specified number of generations. 5.5.9 Prevent reuse of identifiers for a specified number of generations. 7 Y Y Y Supermonent password. 3.5.10 Store and transmit only cryptographically-protected passwords. 3.5.10 Store and transmit only cryptographically-protected		-	'	
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 Restruct, 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 (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (blacklisting) policy to prevent the use of unauthorized software. 3.4.9 Control and monitor user-installed software. 3.5.1 DENTIFICATION AND AUTHENTICATION 3.5.1 Identify system users, processes acting on behalf of users, and devices. 3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prevequisite to allowing access to organizational systems. 3.5.3 Use multifactor authentication for local and network access to privileged accounts. 3.5.4 Employ replay-resistant authentication mechanisms for network access to non-privileged accounts. 3.5.5 Prevent reuse of identifiers for a defined period. 3.5.6 Foreward report and 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 Extra properary password use for system logons with an immediate change to a permanent password. 3.5.10 Store and transmit only cryptographically-protected passwords. 3.5.10 Store and transmit only crypt		Υ	Y	
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 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. 3.5.1 Identify system users, processes acting on behalf of users, and devices. 3.5.1 Identify system users, processes acting on behalf of users, and devices. 3.5.1 Use multifactor authenticate for verify the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems. 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged accounts. 3.5.5 Prevent reuse of identifiers for a defined period. 3.5.6 Prevent reuse of identifiers for a defined period of inactivity. 3.5.7 Enforce a minimum password use for specified number of generations. 3.5.9 Allow the proper parameter of processes of the proper passwords are created. 3.5.9 Prohibit password reuse for a specified number of generations. 4 Y Y A Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y				
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. 3.4.8 Apply deny-by-exception (whitelisting) policy to allow the execution of authorized software. 3.4.9 Control and monitor user-installed software. 3.5.1 DENTIFICATION AND AUTHENTICATION 3.5.1 Identify system users, processes acting on behalf of users, and devices. 3.5.2 Authenticate (or verify the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems. 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged accounts. 3.5.5 Prevent reuse of identifiers for a defined period. 3.5.6 Prevent reuse of 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. 3.5.10 Store a minimum password use for system logons with an immediate change to a permanent password. 3.5.10 Store and transmit only cryptographically-protected passwords. 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 3.6.2 Track, document, and report incidents to designated officials andor authorities 3.6.2 Track, document, and report incidents to designated officials andor authorities 3.6.2 Track, document, and report incidents to designated officials andor authorities 3.6.2 Track, document, and report incidents to designated officials andor authorities 3.6.2 Track, document, and report incidents to designated officials andor authorities		'	'	
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. 3.5.1 DENTIFICATION AND AUTHENTICATION 3.5.1 Identify system users, processes acting on behalf of users, and devices. 3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a pre-requisite to allowing access to organizational systems. 3.5.3 Use multifactor authentication for local and network access to privileged accounts. 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. 3.5.5 Disable identifiers for a defined period. 3.5.6 Disable identifiers after a defined period of inactivty. 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. 3.5.10 Identifiers for a defined period of inactivity. 3.5.10 Identifiers for a defined period of inactivity. 3.5.2 Finforce a minimum password use for system logons with an immediate change to a permanent password. 3.5.5 Disable password reuse for a specified number of generations. 3.5.10 Identifiers for a defined period of inactivity. 3.5.10 Identifiers for a defined period of inactivity. 3.5.2 Finforce a minimum password use for system logons with an immediate change to a permanent password. 3.5.10 Identifiers for a defined period of inactivity. 3.5.10 Identifiers for a defined peri		N	V	
3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. 3.4.8 Apply deep-ty-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. 3.5.1 Identify system users, processes acting on behalf of users, and devices. 3.5.2 Authenticate (or verify the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems. 3.5.4 Employ replay-resistant authentication for local and network access to privileged and non-privileged accounts. 3.5.5 Profroce a minimum password complexity and change of characters when new passwords are created. 3.5.6 Disable identifiers after a defined period of inactivity. 3.5.7 Profroce 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 Provent password use for system logons with an immediate change to a permanent password. 3.5.10 Store and transmit only cryptographically-protected passwords. 3.5.10 Store and transmit only cryptographically-protected passwords. 3.6.10 ISIDENT RESPONSE 3.6.2 Track, document, and report incidents to designated officials andor authorities 3.6.2 Track, document, and report incidents to designated officials andor authorities 3.6.2 Track, document, and report incidents to designated officials andor authorities 3.6.2 Track, document, and report incidents to designated officials andor authorities 3.6.2 Track, document, and report incidents to designated officials andor authorities 3.6.2 Track, document, and report incidents to designated officials andor authorities 3.6.2 Track, document, and report incidents to designated officials andor authorities 3.6.2 Track, document, and report incidents to designated officials andor authorities		IN	'	
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. 3.5.1 DENTIFICATION AND AUTHENTICATION 3.5.1 Identify system users, processes acting on behalf of users, and devices. 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. 3.5.4 Employ replay-resistant authentication mechanisms for network access to 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. 3.6 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.		V	V	We get a let of this by mainly containerizing the applications and
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. 4. Y 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. 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 Ry Problem transmit only cryptographically-protected passwords. 3.5.10 Store and transmit only cryptographically-protected passwords. 3.5.10 Store and transmit only cryptographically-protected passwords. 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 Y		Ť	Y	
software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. 3.49 Control and monitor user-installed software. 3.51 IDENTIFICATION AND AUTHENTICATION 3.5.1 Identify system users, processes acting on behalf of users, and devices. 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. 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 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. 3.6.1 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 Y Y	• • • • • • • • • • • • • • • • • • • •	NI NI	V	
of authorized software. 3.49 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. 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. 3.5.4 Employ replay-resistant authentication mechanisms for network access to 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 a system logons with an immediate change to a permanent password. 3.5.10 Store and transmit only cryptographically-protected passwords. 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 Y Y		IN	l Y	we need to implifient SODO lists to restrict access.
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. 3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a pre-requisite 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. 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. 3.5.5 Prevent reuse of identifiers of 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. 4 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 4 Y Y				
3.5.1 Identify system users, processes acting on behalf of users, and devices. 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. 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 3.6.2 Track, document, and report incidents to designated officials andor authorities Y Y 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.				
3.5.1 Identify system users, processes acting on behalf of users, and devices. 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. 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. 3.5.10 Store and transmit only cryptographically-protected passwords. 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 Y Y		Y	Y	
3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a pre-requisite 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. 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 3.6.2 Track, document, and report incidents to designated officials andor authorities Y 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.				
requisite 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. 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 Y Y				
3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. 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. 3.6.1 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 Y Y I think chile dont require 2FA at the moment Y Not sure we do this now - Cristian Richard Y Y Y Y Y Y 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.		Y	Y	
counts and for network access to non-privileged accounts. 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non- privileged accounts. 3.5.5 Prewent 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. 3.6.1 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 Y Y Not sure we do this now - Cristian Richard Y Y Not sure we do this now - Cristian Richard Y Y A V A V Y A N Y Y A N Y Y A N Y Y A N Y Y A N Y A N Y A N Y A A A A A A A A A A A A	requisite to allowing access to organizational systems.			
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. 3.6.1 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 Y Y Not sure we do this now - Cristian Richard Y A A A A A A A A A A A A	3.5.3 Use multifactor authentication for local and network access to privileged ac-	N	Y	I think chile dont require 2FA at the moment
ileged 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. 3.5.11 Obscure feedback of authentication information. 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 Y 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.	counts and for network access to 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. 3.6.11 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 Y 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.	3.5.4 Employ replay-resistant authentication mechanisms for network access to priv-		Y	Not sure we do this now - Cristian Richard
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. 3.6.11 Closure feedback of authentication information. 3.6.12 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 Y 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.	ileged and non- privileged accounts.			
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. 3.5.11 Obscure feedback of authentication information. 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 Y Y Y	3.5.5 Prevent reuse of identifiers for a defined period.	N	Y	
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. 3.6.1 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 Y 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.	3.5.6 Disable identifiers after a defined period of inactivity.	Υ	Y	
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. 3.6.1 Incident Fesponse 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 Y 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.	3.5.7 Enforce a minimum password complexity and change of characters when new	Υ	Υ	
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. 3.5.10 Doscure feedback of authentication information. 3.6.1 NCIDENT 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 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.	passwords are created.			
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. 3.6.1 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 Y 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.	3.5.8 Prohibit password reuse for a specified number of generations.	Υ	Υ	
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 Y Y Y				
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 Y 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.	, ,,			
3.5.11 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 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.	· · · · · · · · · · · · · · · · · · ·	Υ	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. 3.6.2 Track, document, and report incidents to designated officials andor authorities 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.				
3.6.1 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 Y Y		'	+ '	
that includes preparation, detection, analysis, containment, recovery, and user response activities. 3.6.2 Track, document, and report incidents to designated officials andor authorities Y Y		V	V	ALIDA have incurance which covers this. But we really should be as
sponse activities. 3.6.2 Track, document, and report incidents to designated officials andor authorities Y Y		Ť	1	
3.6.2 Track, document, and report incidents to designated officials andor authorities Y Y				contract to look over logs etc. to note when we are nit.
	·	V	- V	
DOLITIMETHAL AND EXTERNAL TO THE ORGANIZATION.		Ť	1	
	both internal and external to the organization.		1	



3.6.3 Test the organizational incident response capability.	N	Υ	
3.7 MAINTENANCE			
3.7.1 Perform maintenance on organizational systems.	Υ	Y	
3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to	Y	Y	
conduct system maintenance.			
3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Υ	Y	
3.7.4 Check media containing diagnostic and test programs for malicious code before	Υ	Y	
the media are used in organizational systems.			
3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions		Y	Cristian Richard
via external network connections and terminate such connections when nonlocal			
maintenance is complete.			
3.7.6 Supervise the maintenance activities of maintenance personnel without re-	Υ	Y	
quired access authorization.			
3.8 MEDIA PROTECTION			
3.8.1 Protect (i.e., physically control and securely store) system media containing CUI,	N	Y	
both paper and digital.			
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	Υ	Y	
reuse.			
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	Υ	Y	
during transport outside of controlled areas.	·	'	
3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI	N	Y	
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.		Y	Cristian Richard
3.8.8 Prohibit the use of portable storage devices when such devices have no identi-	Υ	Y	Cristian Menard
fiable owner.	'	'	
3.8.9 Protect the confidentiality of backup CUI at storage locations.	Υ	Y	
3.9 PERSONNEL SECURITY	'	'	
3.9.1 Screen individuals prior to authorizing access to organizational systems contain-	Υ	Y	Only project team members will have access to CUI - all are know in-
ing CUI.	1	'	dividuals. This doe snot suggest backgroung security screening and
ing Coi.			it was also explicitly not requireed by the agencies in seciton 2 of the
			requirements document.
3.9.2 Ensure that organizational systems containing CUI are protected during and af-	Υ	Y	requirements documents
ter personnel actions such as terminations and transfers.	·	'	
3.10 PHYSICAL PROTECTION			
3.10.1 Limit physical access to organizational systems, equipment, and the respective	Υ	Y	This physical access limitaitons will increase with locks on server cab-
operating environments to authorized individuals.	·	'	inets etc. but key card access is already in place.
3.10.2 Protect and monitor the physical facility and support infrastructure for organi-	Υ	Y	Security is in place on Cero Pachon and at the entrace to the moun-
zational systems.	·	'	tain - though not only for Rubin so not permanently at the observa-
Zutional Systems.			tory.
3.10.3 Escort visitors and monitor visitor activity.	Y	Y	Actual visitors are escorted on the summit - contractors are consid-
3.10.3 Escore visitors and monitor visitor activity.	·	'	ered more like staff.
3.10.4 Maintain audit logs of physical access.		Y	Crisitian - does the key card system keep an audit ?
3.10.5 Control and manage physical access devices.	Y	Y	erisitati does tre key eard system keep arradate.
3.10.6 Enforce safeguarding measures for CUI at alternate work sites.	Y	Y	This brings in ? and ?. We not the use of OnePasseword - we do not
3.10.0 Efficice saleguarding measures for Corat alternate work sites.	'	'	write security codes on paer and put them in a fireproof safe.
3.11 RISK ASSESSMENT			white security codes on paer and put them in a meproor sale.
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 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 effec-			
tiveness of the controls.			
aveness of the controls.			



2.12.4 Develop degree and pariedically under a setum acquirty plane that de	I		
3.12.4 Develop, document, and periodically update system security plans that de-			
scribe system boundaries, system environments of operation, how security require-			
ments are implemented, and the relationships with or connections to other sys-			
tems.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 organiza-			
tional 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 communi-			
cations traffic by exception (i.e., deny all, permit by exception).			
3.13.7 Prevent remote devices from simultaneously establishing non-remote connec-			
tions 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 safe-			
guards.			
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 or-			
ganizational 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.	Υ	Υ	Currently we have no mobile code
3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technolo-			
gies.			
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.	Υ	Υ	
3.14.2 Provide protection from malicious code at designated locations within organi-	N	N	
zational systems.			
3.14.3 Monitor system security alerts and advisories and take action in response.	Υ	Y	
3.14.4 Update malicious code protection mechanisms when new releases are avail-	Y	Y	
able.		'	
3.14.5 Perform periodic scans of organizational systems and real-time scans of files	Υ	Y	
from external sources as files are downloaded, opened, or executed.		'	
3.14.6 Monitor organizational systems, including inbound and outbound communi-	Υ	Y	
cations traffic, to detect attacks and indicators of potential attacks.	'	'	
Total requirements		108	
•			
Total Rubin Intends to comply with		87	
Total Rubin Complies with in 2021		58	

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
AURA	Association of Universities for Research in Astronomy
AVS	Alert Vetting System
CPU	Central Processing Unit
CUI	Controlled Unclassified Information
DM	Data Management
DMTN	DM Technical Note
DOE	Department of Energy
FTE	Full-Time Equivalent
IP	Internet Protocol
IT	Information Technology
LHN	long haul network
LLNL	Lawrence Livermore National Laboratory
LSE	LSST Systems Engineering (Document Handle)
NIST	National Institute of Standards and Technology (USA)
NSF	National Science Foundation
OPS	Operations
OSS	Observatory System Specifications; LSE-30
POSIX	Portable Operating System Interface
RAID	Redundant Array of Inexpensive Disks
SLAC	SLAC National Accelerator Laboratory



ТВ	TeraByte
VPN	virtual private network
deg	degree; unit of angle