

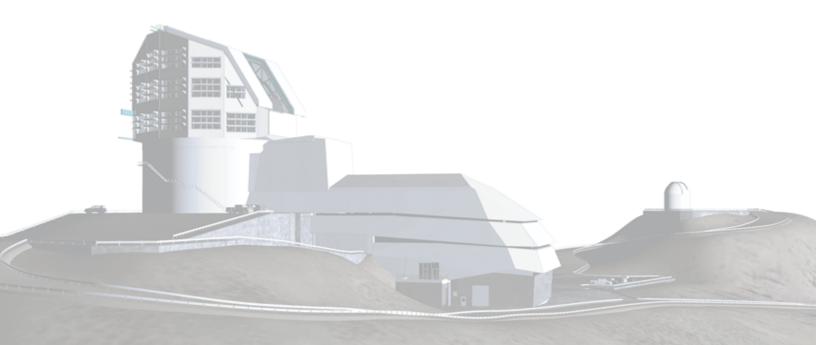
# Vera C. Rubin Observatory Data Management

# 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: 2021-07-23





# **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	4
	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	5
4	Conclusion	5
Α	Compliance with NIST Standard	5
В	References	9
C	Acronyms	9



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

# 3 Response to the requirements

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

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

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

<sup>&</sup>lt;sup>1</sup>{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.



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			
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 <sup>2</sup>. We will need to have one at SLAC and one at Chile for redundancy to ensure no data loss.

With the commissioning constraint that means this needs to be a 30 day store for Full images and engineering data looking at DMTN-135 table table 40 this comes out to about 500TB of usable disk. Table 4 gives the cost calculation or this.

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

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

# 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

<sup>&</sup>lt;sup>2</sup>https://min.io/product/enterprise-object-storage-encryption



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.			, g
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	Υ	This is our policy.
data after a period of inactivity.	<u> </u>		
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	Y	Cristian - not sure if we do this now
3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote ac-	Υ	Y	VPN is in use
cess sessions.			
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	Υ	
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	Y	
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	Y	Y	CUI will not exist on mobile devices - in the case where an image may exist on say commissioning team laptop we will have disk encryption enabled.
3.1.20 Verify and controllimit connections to and use of external systems.	Y	Y	This implies vetting of devices that connect to the control network - we use mac address for laptops and personal mobile phones can not connect to the control network.
3.1.21 Limit use of portable storage devices on external systems.	N	Y	CristianRichard - impliesn no USB drives etc enabled
3.1.22 Control CUI posted or processed on publicly accessible systems.	Υ	Υ	We do not intend to post CUI on publicly accessible systems.
3.2 AWARENESS AND TRAINING			
3.2.1 Ensure that managers, systems administrators, and users of organizational sys-	Υ	Y	
tems are made aware of the security risks associated with their activities and of the			
applicable policies, standards, and procedures related to the security of those sys-			
tems.			
3.2.2 Ensure that personnel are trained to carry out their assigned information	N	Y	
security-related duties and responsibilities.			
3.2.3 Provide security awareness training on recognizing and reporting potential in-	Y	Υ	We would like to do more here like capture flag exercises for devel-
dicators of insider threat.			opers.
3.3 AUDIT AND ACCOUNTABILITY			
3.3.1 Create and retain system audit logs and records to the extent needed to enable	Υ	Υ	
the monitoring, analysis, investigation, and reporting of unlawful or unauthorized sys-			
tem activity.		1	
3.3.2 Ensure that the actions of individual system users can be uniquely traced to	Υ	Υ	
those users, so they can be held accountable for their actions.		1	
3.3.3 Review and update logged events.	P	Y	We may look for a third party contract for this.
3.3.4 Alert in the event of an audit logging process failure.	N	Y	
3.3.5 Correlate audit record review, analysis, and reporting processes for investigation	N	Y	Again shall look for third party contract for this
and response to indications of unlawful, unauthorized, suspicious, or unusual activity.			
3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.	N	Y	
3.3.7 Provide a system capability that compares and synchronizes internal system	Υ	Y	
3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.			



As 3 Limit management of audit liggarg furntransity to a subset of privileged users.  3.4 CONGRIGHON MANAGEMENT  3.4 CONGRIGHON MANAGEMENT  3.4 CONGRIGHON MANAGEMENT  3.4 CONGRIGHON MANAGEMENT  4.5 Element of a maintain baseline configurations and invertories of organizational years.  4.4 Element of a maintain baseline configurations and invertories of organizational years.  4.4 Text. review of a maintain baseline configurations setting for micromometeronogy of the respective gotest in development life cycles.  4.5 Text. review opens or disappress, and log changes to organizational years.  4.4 Text. review opens or disappress, and log changes to organizational years.  4.5 Text. review opens or disappress, and logical access restrictions, associated with changes to organizational systems.  4.5 Defined note exercity maint a place which also cover them.  4.5 Defined note exercity maint a place which also cover the infrastructure as code.  4.5 Defined note exercity maint a place which also cover them.  4.5 Defined note exercity maintain a place which also cover the infrastructure as code.  4.5 Defined note exercity maintain a place which also cover the infrastructure as code.  4.5 Defined note exercity maintain a place which also cover the infrastructure as code.  4.5 Defined note exercity maintain a place which also cover the infrastructure as code.  4.5 Defined note exercity maintain a place which also cover the infrastructure as code.  4.5 Defined note in a place which also cover the infrastructure as code.  4.5 Defined note in a place which also cover the infrastructure as code.  4.5 Defined note in a place which also cover the infrastructure as code.  4.5 Defined note in a place which also cover the infrastructure as code in a place which also cover the place of the infrastructure as code in a place which also cover the infrastructure as code in a place which also cover the place of the infrastructure as code in a place which also cover the infrastructure as code in a place which also cover the infrastructure	3.3.8 Protect audit information and audit logging tools from unauthorized access,	Υ	Υ	
3.4 Establish and manus baseline configurations and inventions of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system divelopment life (system).  3.4 Establish and enforce security configuration settings (system).  3.4 Establish and enforce security configuration settings).  3.4 Establish and enforce security configuration settings (system).  4.4 Establish and enforce security configuration settings).  3.4 Establish and enforce security configuration settings (system).  4.4 Establish and enforce security configuration settings).  3.4 Establish and enforce security configuration settings.  4.4 Establish and enforce security configuration settings.  5.4 And explore security in security of the security of security security of the security of security security of the security of substitution of early security security.  5.4 Establish and enforce security as ode.  5.4 Establish and enforce security security of the security of substitution of early security security of the security of explores security security of the security of explores security	modification, and deletion.			
3.4 Establish and markatin baseline configurations and inventions of organizational systems including invalves, software (increased and provided the respective system development (if cycles, add. Establish and devices score), organizational systems, and construction of the provided in cycles and cycles of the cycles and cycles of the provided in cycles and cycles of the provided in cycles and cycles of the provided in cycles and cycles of the cycles and cycles of the provided in cycles and cycles of the cycles and cycles of the informaticurure as rode.  3.4.4 Analyse the security impacts of cycles and cycles of the cycles and cycles of the informaticurure as rode.  3.4.5 Established only cycles of the cycles and cycles of the cycles and cycles of the cycles and cycles of the informaticurure as rode.  3.4.6 Engly they be precised of explosition and policy of cycles and cycles of the cycles and cy		Υ	Υ	
systems (including hardware, software, firmware, and decumentation) throughout the respective system development the cycles.  3.4.2 Statishi and enforce security configuration settings for information technology or product amplication in organizational systems.  3.4.3 Tack, review, approve or disapprove, and legical access resprictions or security configuration settings for information and security or setting the product and security or disapprove, and enforce physical and logical access resprictions or security or setting the principle of seat functionally systems.  3.4.5 Entrylight the principle of seat functionally systems, and security setting the principle of seat functionally systems, and security setting systems are setting seat functionally systems, and security setting systems are setting seat functionally systems, and security setting systems are setting seat functionally systems, and security setting seat functionally systems, and security setting seat functionally systems, and seat functionally systems and seat functionally systems are seat for seat functionally systems, and seat functionally systems are seat for seat functionally systems and systems.  3.4.6 Entrylight setting seat functionally systems, seat functional systems,				
the respective gyatem development life cycles.  Al 2 Establish and efforce security conjugation settings for information sectionally products employed in organizational systems.  Al 3 Tarks, revisit, approve of slappower, and lag changes to organizational system (in the infrastructure as code.)  Al 4 Analyst the security impact of changes prior to implementation.  Al 5 Define, document, approve, and significant organizational systems (in the infrastructure as code.)  Al 6 Analyst the security impact of changes prior to implementation.  Al 6 Finefrey the process of the infrastructure as code.  Al 7 Establish and process of the infrastructure as code.  Al 7 Establish and the use of nonesential programs, functions, ports, to provide only essential capabilities.  Al 7 Establish and less or prevent the use of nonesential programs, functions, ports, to provide only essential capabilities.  Al 7 Establish and less or prevent the use of nonesential programs, functions, ports, to provide only essential capabilities.  Al 8 Apply deny-exception (blacklisting) policy to prevent the use of unauthorized software or deny-sit, permit-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-sit, permit-by-exception (blacklisting) policy to allow the execution of authorized software or deny-sit, permit-by-exception (blacklisting) policy to allow the execution of authorized software user installed rofluence.  Al 8 Apply deny-exception (blacklisting) policy to prevent the use of unauthorized software or deny-sit, permit-by-exception (blacklisting) policy to allow the execution of authorized software user installed rofluence.  Al 8 Apply deny-exception (blacklisting) policy to allow the execution of authorized software user installed rofluence.  Al 8 Apply deny-exception (blacklisting) policy to prevent the use of unauthorized software user or deny-sit permit of unauthorized software user or deny-sit permit of unauthorized software user or deny-sit permit of unauthorized software user or deny-sit permi		Υ	Y	
3.4.2 Facts and an enforce security configuration estimates for information technology of products employed in organizational systems. 3.4.3 Facts, review, approve or disapprove, and log changes to organizational system. 3.4.4 Analyze the security impact of changes prior to implementation. 3.4.4 Analyze the security impact of changes prior to implementation. 3.4.4 Analyze the security impact of changes prior to implementation. 3.4.5 Define, document, approve, and inforce physicial and logical access restrictions associated with changes to organizational systems. 3.4.7 Security impact of changes prior to implementation. 3.4.8 Apply deny by exception (blocklisting policy to prevent the use of nonauthorized protections of authorized software. 3.4.8 Security impact of changes prior to implementation of authorized software. 3.4.9 Central and implementation policy in the dentities of users, processes, or devices, as a previous protection of authorized software. 3.5 INDEPTIBER/IDENTIFE/IDENT				well tracked. IT inventory all the hardware.
Jordon Exposure of in organizational systems.  As 3-1 Track, revoke, approve of disengance, and log danges to organizational system.  As 3-1 Track, revoke, approve of segregory, and log danges to organizational system.  As 4-1 Analyze the security impact of changes prior to implementation.  As 4-2 Prior, document, approve, and enforce physical and logical access restrictions.  As 4-2 Prior, document, approve, and enforce physical and logical access restrictions.  As 4-2 Prior, document, approve, and enforce physical and logical access restrictions.  As 4-2 Prior, document, approve, and enforce physical and logical access restrictions.  As 4-2 Prior, document, approve, and enforce physical and logical access restrictions.  As 4-2 Prior, document, approve, and enforce physical and logical access restrictions.  As 4-2 Prior, document, approve, and enforce physical and logical access and access and approximately segment of the security of the physical access.  Y  We see a lot of the lyminity containers and horizons, and services.  As 4-2 Prior, document, approve access to prior logical programs, functions, ports, and protocols, and services.  As 4-2 Prior, document, approve access to expensional physical policy to allow the execution of authorized software.  As 5-3 Eneminated and access to expensional experiment.  As 5-3 Eneminated and access to expensional systems.  As 5-3 Eneminated and access to expensional systems.  As 5-3 Eneminated and Asia Asia Asia Asia Asia Asia Asia Asia				
3.43 Tack, review, approve of disapprove, and fig. changes to organizational system. 3.44 Analyze the security impact of changes prior to implementation. 3.45 Define, document, approve, and force physical and logical access restrictions, associated with changes to organizational systems. 3.45 Define, document, approve, and force physical and logical access restrictions, associated with changes to organizational systems. 3.46 Employ the reproject of cest functionally by certifiquing eigenizational systems. 3.46 Employ the reproject of cest functionally by certifiquing eigenizational systems. 3.46 Employ dening the execution of the system deposition of the system d		Υ	Y	
tems.  4.4. Analyse the security impact of changes prior to implementation.  5.4.5 Enfire, document, approxe, and enforce physical and lagical access restrictions of a 3.4.5 Enfire, document, approxe, and enforce physical and lagical access restrictions of a 3.4.6 Employ the principle of feast functionally systems.  5.4.6 Employ the principle of feast functionally systems or protected, and secured acqualities.  5.4.7 Restrict, disable, or prevent the use of nonesternial programs, functions, ports, portionally and security of the protection of authorized buttons or in deny all, permit by exception whitelesting policy to allow the execution of authorized buttons or in deny all, permit by exception whitelesting policy to allow the execution of authorized buttons or intervent access.  5.4 Destriction AND AUTHENTICKTON  5.5 Illentify system users processes acting on behalf of users, and devices.  5.5 Authenticator or verify the elements of ouces, processes, or devices, a a pre-vision of the protection of the p				
3.4.3 Se Pelins, Centured, approve, and entering Periparial and logical access restrictions associated with changes to organizational systems. 3.4.5 Pelins, for principle of least functionality by configuring 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, disabilities, the second organizational programs, functions ports, by the provide only essential capabilities, and protocols, and services. 3.4.8 Apply deeply exception (blackdisting) policy to prevent the use of unauthorized software or deny-all, permit by-exception (blackdisting) policy to prevent the use of unauthorized software or deny-all, permit by-exception (blackdisting) policy to allow the execution of authorized software. 3.4.8 Control and monitor user-disabilities of software. 3.4.8 Control and monitor user-disabilities of software. 3.5.1 Authorization (or verify the identities of users, processes, or devices, as a previous) and protocols. 3.5.2 Authorization (or verify the identities of users, processes, or devices, as a previous) and protocols of the protocol or software or soft		Υ	Y	= ' '
3.4.5 Employ the principle of least functional joystems. 3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only expendent of apathlitis. 3.4.7 Restrict, disable, or prevent the use of nonesertial 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 (blacklisting) policy to prevent the use of unauthorized software. 3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software. 3.4.9 Central and monitor user installed software. 3.5 DENTIFICATION AND AUTHENTICATION 3.5 DENTIFICATION AND AUTHENTICATION 3.5 Intentify separation provided in the providence of users, processes, or devices, as a preventive to allowing access to organizational systems. 3.5.3 Demailification authentication for local and network access to privileged access to expensional providence of allowing access to expensional systems. 3.5.5 Employer representation authentication by the intention of excess to privileged access to privileged access to expensional systems. 3.5.5 Employer representation authentication by the foreign and network access to privileged access to expensional systems. 4.5.5 Employer representation authentication by the foreign and network access to privileged and non-prolleged accounts. 3.5.5 Prevent representation authentication and the period of inactivity. 4.7.5 Employer representation authentication and the period of inactivity. 4.7.7 Expensional province of inactivity. 4.7.7 Expensional inactivity and the period of inactivity. 4.7.8 Femployer representation and the period of inactivity. 4.7.9 Femployer antiferral set or a defined period of inactivity. 4.7.9 Femployer authentication and the period of inactivity. 4.7.9 Femployer antiferral province and the period of inactivity. 4.7.9 Femployer antiferral province and the period of inactivity. 4.7.9 Femployer antiferral province and the period of inactivity. 4.7.9 Femp				the infrastructure as code.
As Exempley frompley of least functionality by configuring organizational systems to provide only essential capabilities.  A) A Empley the principle of least functionality by configuring organizational systems to provide only essential capabilities.  A) A Restrict, fashles, or prevent the use of nonessential programs, functions, ports, protected systems or deny all, permit by exception (blackdisting) policy to prevent the use of unauthorized software or deny all, permit by exception (whitefibility) policy to allow the execution of authorized software or deny all, permit by exception (whitefibility) policy to allow the execution of authorized software.  3.45 Centrol and monitor user installed software.  3.5 Internity system users, processes acting on behalf of users, and devices.  3.5 Internity system users, processes acting on behalf of users, and devices.  4. Y  4. Y  4. Y  4. Y  4. Y  4. Y  4. Inthiniciplish don't require 2FA at the moment counts and for network access to privileged accounts.  5.5 Employ replayer essistant authentication for local and network access to privileged accounts.  5.5 Event reuse of identifiers for a defined period.  5.5 Possible internities ster a defined period.  5.5 Possible internities ster as defined period.  5.5 Possible internities ster as defined period of macrotivity.  5.5 Possible internities ster as defined period of macrotivity.  5.5 Possible internities ster as defined period of macrotivity.  5.5 Possible internities ster as defined period of macrotivity.  5.5 Possible internities ster as defined period of macrotivity.  5.5 Possible internities ster as defined period of macroticity.  5.5 Possible internities ster as defined period of macroticity.  5.5 Possible internities ster as defined period of macroticity.  7. Y  8.5 Possible internities ster as defined period of macroticity.  8.5 Possible internities ster as defined period of macroticity.  9. Y  9				
1.4.6 Employ the principle of least functionality by configuring organizational systems on provide only agressivated apabilities.  3.4.7 Restrict, disable, or prevent the use of nonescential programs, functions, ports.  3.4.8 Apply deny by exception thiskisting policy to prevent the use of unauthorized software or deny-light permit-by-exception (whitelisting) policy to prevent the use of unauthorized software.  3.4.8 Apply deny by exception thiskisting policy to prevent the use of unauthorized software.  3.4.9 Control and monitor user installed software.  3.5 IORITION AND AUTHORICATION  4.5 IORITION AUTHORICATION  4.5		Y	Y	
to provide only essential capabilities.  A) A Restrict, dabbie; or prevent the use of nonessential programs, functions, ports, y and protocols, and services.  A) A Reply dropty-pocception (biblicisting) policy to prevent the use of unauthorized of authorized software or deny all, permit by exception (while/sising) policy to allow the execution of authorized software.  A) A Control and monitor user-installed software.  A) A Control and monitor user-installed software.  A) S Control and monitor user-installed software.  A) S Control and monitor user-installed software.  A) S Control and monitor user-installed software.  A) Y Y V P P P P P P P P P P P P P P P P P				
3.4.3 Reptire, disable, or prevent the use of nonescential programs, functions, ports.  Y Y Y We get all of this by mainity containerizing the applications and having users work with the ymainity containerizing the applications and having users work with the ymainity containerizing the applications and having users work with the ymainity containerizing the applications and having users work with the ymainity containerizing the applications and shortware of deny, and provided the cecurion of authorized software.  3.4.9 Control and monitor user-installed software.  3.5.10 Entity symmut users, processes acting on behalf of users, and devices.  3.5.11 Identify symmut users, processes acting on behalf of users, and devices.  3.5.2 Employ replay-resistant authentication for local and network access to privileged account.  3.5.3 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged account.  3.5.5 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged account.  3.5.5 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged account.  3.5.5 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged account.  3.5.5 Employ replay-resistant authentication inclination and period of incitivity.  3.5.5 Employ replay-resistant authentication incitivity.  4.7 Y  4.7 Y  4.7 Y  4.7 Y  4.7 Not sure we do this now - Cristian Richard  4.8 Septimentifiers after a defined period of incitivity.  4.7 Y  4.7		N	Y	
protocols, and services.  Als Alp Apply deny-physocreption (balcistizing) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.  3.43 Control and monitor user-installed software.  3.45 Control and monitor user-installed software.  3.54 DENTIFICATION AND AUTHORICATION  3.51 Identify system users, processes acting on behalf of users, and devices.  4.7 Y Y P Y P Y P Y P Y P Y P Y P Y P Y P				
3.4.3 Apply derry by exception (blacklisting) policy to allow the execution of authorized software.  3.5.10 Employ (apply apply appl		Υ	Y	, , , , , , , , , , , , , , , , , , , ,
software or deriy-all, permit-by-exception whitelistingly policy to allow the execution of outhorized software.  3.4.9 Control and monitor user-installed software.  3.5.1 Control and monitor user-installed software.  3.5.1 Control and monitor user-installed software.  3.5.2 Authoritical row verify the identifies of users, and devices.  3.5.3 Latentifies for verify the identifies of users, processes, or devices, as a previous to allowing access to organizational systems.  3.5.3 Latentifies for verify the identifies of users, processes, or devices, as a previous to allowing access to organizational systems.  3.5.3 Latentifies for a verified for information or rectified and non-privileged accounts.  3.5.4 Employ register authoritical for for local and network access to privileged accounts.  3.5.5 Premet rese of identifiers for a defined period.  3.5.5 Premet rese of identifiers for a defined period.  3.5.5 Premet rese of identifiers for a defined period.  3.5.5 Premet rese of identifiers for a defined period.  3.5.6 Premet rese of identifiers for a defined period.  3.5.6 Premet rese of identifiers for a defined period.  3.5.7 Entire rese of identifiers for a setting of inactivity.  4.7 V.	•			1 1
of authorized software.  3.4.9 Control and monitor user-installed software.  Y Y Y  3.5.1 POINTIFICATION AND AUTHENTICATION  3.5.2 Authenticals for verify the identifies of users, processes, or devices, as a pre- requisite to allowing access to organizational systems.  3.5.3 Linetify system users, processes acting on behalf of users, and devices.  Y Y  Substitution of the intervention of the interventio		N	Y	We need to implment SUDO lists to restrict access.
3.5 IDENTIFICATION AND AUTHORITORION AUTHORITORION AND AUTHORITORION AND AUTHORITORION AND AUTHORITORION AND AUTHORITORION AUTH				
3.5.1 Identify spetm users, processes acting on behalf of users, and devices.  3.5.2 Authenticate for verify the identities of users, processes, or devices, as a pre- requisite to allowing access to organizational systems.  3.5.3 User multifactor authentication for local and network access to privileged ac- counts 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 Pewnet result authentication mechanisms for network access to privileged accounts.  3.5.6 Pemploy replay-resistant authentication mechanisms for network access to privileged accounts.  3.5.7 Employer replay-resistant authentication mechanisms for network access to privileged accounts.  3.5.8 Pewnet result of the privileged accounts.  3.5.9 Pewne			1	
3.5.1 Elemity system users, processes acting on behalf of users, and devices. 3.5.2 Authenticate for verify the dentities of users, processes, or devices, as a pre-requisite to allowing access to organizational systems. 3.5.3 Lise multifactor authentication for local and network access to privileged accounts and for network access to one-privileged accounts. 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and network access to non-privileged accounts. 3.5.5 Employ replay-resistant authentication mechanisms for network access to privileged and network access to non-privileged accounts. 3.5.5 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. 3.5.5 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. 3.5.5 Employ replay-resistant authentication mechanisms for network access to privileged accounts. 3.5.5 Employ replay-resistant authentication mechanisms for network access to privileged accounts. 4 V V V V V V V V V V V V V V V V V V V		Υ	Y	
3.5.2 Limberticate (or verify) the identities of users, processes, or devices, as a pre- requisite to allowing access to againational systems. 3.5.3 Use multifactor authentication for local and network access to privileged ac- counts and for network access to non-privileged accounts. 3.5.4 Employ replayer-resistant authentication mechanisms for network access to priv- ileged and non-privileged accounts. 3.5.5 Frenter uses 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 Problem password ruse for system logons with an immediate change to paramaneth password. 3.5.9 Provent replayer for a pecified number of generations. 3.5.9 Provent replayer for a pecified number of generations. 3.5.9 Provent replayer for a pecified number of generations. 3.5.9 Provent replayer for a pecified number of generations. 3.5.9 Provent replayer for a pecified number of generations. 3.5.9 Provent replayer for a pecified number of generations. 3.5.9 Provent replayer for a pecified number of generations. 3.5.9 Provent replayer for a pecified number of generations. 3.5.9 Provent replayer for a pecified number of generations. 3.5.9 Provent replayer for a pecified number of generations. 3.5.9 Provent replayer for a pecified number of generations. 3.5.9 Provent replayer for a pecified number of generations. 3.5.10 Discours for transmit only cryptographically protected passwords. 3.5.10 Discours for transmit only cryptographically protected passwords. 3.5.11 Obscure foredback of authentication information. 3.6.11 Obscure feedback of authentication information. 3.6.1 Track footomy for period provent period pro				
requisite to allowing access to organizational systems.  5.3.1 Sue multifactor authentication for local and network access to privileged accounts.  5.3.4 Employ replayer esstart authentication mechanisms for network access to privileged and non-privileged accounts.  5.3.5 Prevent reuse of identifiers for a defined period.  5.5.6 Disable identifiers after a defined period.  5.5.6 Disable identifiers after a defined period in incivity.  5.5.7 Enforce a minimum password complexity and change of characters when new your passwords are created.  5.5.8 Prohibit password reuse for a specified number of generations.  5.5.9 Allow temporary password use for system logons with an immediate change to your parameter password.  5.5.10 Store and transmit only cyptographically-protected passwords.  5.6.1 Tost, force an imminum password complexity and change of characters when new your passwords are created.  5.6.1 Tost, force a minimum password complexity and change of characters when new your your passwords are created.  5.5.8 Prohibit password reuse for a specified number of generations.  7.7 Your your password and transmit only cyptographically-protected passwords.  7.8 Your your password and transmit only cyptographically-protected passwords.  7.9 Your your password of a period password of the passwords are repeated.  8.6.1 Tost, force feedback of authentication information.  8.6.2 Track, document, and report incidents to designated officials andor authorities your passwords are report incidents to designated officials andor authorities your passwords are password.  8.6.2 Track, document, and report incidents to designated officials andor authorities your your password in the password of your your passwords are password.  8.6.2 Track, document, and report incidents to designated officials andor authorities your your password your p				
3.5.3 Emblish comparing password complexity and change of characters when new passwords are created.  3.5.4 Employ replay-resistant authentication mechanisms for 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.  N Y Y S.5.5 Prevent reuse of identifiers for a defined period.  N Y Y S.5.5 Prevent reuse of identifiers for a defined period of inactivity.  Not sure we do this now - Cristian Richard  1.5.6 Prevent reuse of identifiers after a defined period of inactivity.  Not sure we do this now - Cristian Richard  1.5.7 Enforce a minimum password complexity and change of characters when new password reuse for a specified number of generations.  1.5.8 Prohibit password reuse for a specified number of generations.  1.5.9 Prevent reuse for a specified number of generations.  1.5.10 Store and transmit only cryptographically-protected passwords.  1.5.10 Store and transmit only cryptographically-protected passwords.  1.5.11 Discurs feedback of authentication information.  1.5.12 Store and transmit only cryptographically-protected passwords.  1.5.13 Store and transmit only cryptographically-protected passwords.  1.5.14 Store period response control incident-handling capability for organizational systems that includes preparation, decreasing a minimum password reuse of the control of the cont		Υ	Y	
Lounts 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 passwords use for system logons with an immediate change to a permanent password.  3.5.9 Allow temporary passwords 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 Obscrive feedback of authentication information.  4 Y Y  4 AURA have insurance which covers this. But we really should have a contract to look over logs etc. to note when we are hit. sponse activities.  3.6.1 Establish an operational incident handling capability.  3.6.2 Track, document, and report incidents to designated officials andor authorities but hinterial and external to the organization.  3.6.3 Test the organizational incident response capability.  3.7.1 Penform maintenance on organizational systems.  3.7.2 Penform maintenance on organizational systems.  3.7.3 Fency equipment removed for off-site maintenance is santized of any CUI.  3.7.3 Fency equipment removed for off-site maintenance is santized of any CUI.  3.7.3 Fency equipment removed for off-site maintenance is santized of any CUI.  3.7.3 Fency equipment removed for off-site maintenance is santized of any CUI.  3.7.4 Check maintenance activities of maintenance personnel without required access authorization.  3.7.5 Expective the maintenance activities of maintenance personnel without required access authorization.  3.8 MEDIA PROTECTION  3.8 Instruction to establish nonlocal maintenance sessions  4 Y  5 Y  5 Y  5 Y  5 Y  5 Y  5 Y  5 Y				
3.5.4 Foreign propriety estistant 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. 3.5.6 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 Prohibits password reuse for a specified number of generations. 3.5.8 Prohibits password reuse for a specified number of generations. 3.5.8 Prohibits 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 proparation, detection, analysis, containment, recovery, and user response activities. 3.6.2 Track, document, and report incidents to designated officials andor authorities by the internal and external to the organizational incident response capability. 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance on organizational systems. 3.7.5 Require media contraining diagnostic and test programs for mailicious code before the media complicational systems. 3.7.6 Supervise the maintenan	1 9	N	Y	I think chile dont require 2FA at the moment
lleged and non-privileged accounts.  3.5.5 Prevent reuse of identifiers for a defined period.  3.5.6 Disable identifiers are 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 y a permanent password.  3.5.10 Store and transmit only cryptographically-protected passwords.  3.5.10 Store and transmit only cryptographically-protected passwords.  3.5.11 Obscure feedback of authentication information.  3.6.11 Stabilish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.  3.6.12 Stabilish an operational incident sto designated officials andor authorities both internal and external to the organization.  3.6.3 Fast the organizational incident response capability.  3.7.1 Perform maintenance on organizational systems.  3.7.2 Perform maintenance on organizational systems.  3.7.3 Forvide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance or off-site maintenance is sanitized of any CUI.  3.7.3 Forvide controls on the tools, techniques, mechanisms, and personnel used to young the maintenance of organizational systems.  3.7.4 Check media containing diagnostic and test programs for mailicous code before the media are used in organizational systems.  3.7.5 Enguine maintenance activities of maintenance personnel without required access authorization.  3.8 MEDIA PROTECTION  3.8 MEDIA PROTECTION  3.8 JEDIA PROTECTION  4.7 We understand we should label rooms and machines according to https://www.archives.gov/filescu/2016/1206-cui-marking-handbook to https://www.archives.gov/filescu/2016/1206-cui-marking-handbook to https://www.archives.gov/filescu/2016/1206-cui-marking-handbook to https://www.archives.gov/filescu/2016/1206-cui-marking-handbo	i i			
3.5.6 Disable Identifiers for a defined period.  8. N. Y. 3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.  9. Y. Y. 3.5.8 Prohibit password ruse for a specified number of generations.  9. Y. Y. 3.5.9 Robinity password use for a specified number of generations.  9. Y. Y. 3.5.9 Allow temporary password use for system logons with an immediate change to paramanent password.  9. S.5.10 Store and transmit only cryptographically-protected passwords.  9. Y. Y. 9. Y. Y. 9. Y.			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. 3.5.10 Store and transmit only cryptographically-protected passwords. 3.5.11 Obscure feedback of authentication information. 3.6.11 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 both internal and external to the organization. 3.6.3 Test the organizational incident response capability. 3.7.4 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance on organizational systems. 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Enguine multifactor authentication to establish nonlocal maintenance was cultion granizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8.1 Establish connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Equire or district system media containing CUI, but paper and digital. 3.8.1 Establish connections and machines according to https://www.archives.gorfilescui20161206-cui-marking-handbook-				
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. 4.5.9 Allow temporary password use for system logons with an immediate change to a permanent password. 5.5.10 Store and transmit only cryptographically-protected passwords. 5.5.10 Store and transmit only cryptographically-protected passwords. 5.5.11 Obscure feedback of authentication information. 5.5.11 Obscure feedback of authentication information. 7.7 Y 7.7 AURA have insurance which covers this. But we really should have a contract to look over logs etc. to note when we are hit. 5.6.2 Track, bocument, and report incidents to designated officials andor authorities both internal and external to the organization. 5.6.2 Track, bocument, and report incidents to designated officials andor authorities both internal and external to the organization. 5.6.3 Test the organizational incident response capability. 7.7 MAINTENANCE 7.7 MAINTENANCE 7.7 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance on organizational systems. 7.9 Y 7.7 Cristian incident removed for off-site maintenance is sanitized of any CUI. 7.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 7.7.5 Require multifactor authentication to establish nonlocal maintenance assisting a submit of the maintenance activities of maintenance when nonlocal maintenance is complete. 7.7.5 Supervise the maintenance activities of maintenance personnel without required access authorization. 7.8.1 MEDIA PROTECTION 7.8.2 Limit access to CUI on system media to authorized users. 7.9 V use understand we should label rooms and machines acording to https://www.archives.go/filescui2/0161206-cui-marking-handbook.	'			
passwords are created.  3.5.8 Prohibit password use for a specified number of generations.  5.5.9 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.  7. Y. Y. Y. S.5.11 Obscure feedback of authentication information.  8.6 INCIDENT RESPONSE  8.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.  8.6.2 Track, document, and report incidents to designated officials andor authorities both internal and external to the organization.  8.6.3 Test the organizational incident response capability.  8.7.4 MAINTENANCE  8.7.3.7 Perform maintenance on organizational systems.  9. Y.				
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. 3.5.11 Obscure feedback of authentication information. 3.5.11 Obscure feedback of authentication information. 3.6.1 Stabilish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. 3.6.2 Track, document, and report incidents to designated officials andor authorities both internal and external to the organization. 3.6.3 Test the organizational incident response capability. 3.7.1 Perform maintenance on organizational systems. 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to ronduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions as external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.  N Y We understand we should label rooms and machines acording to https://www.archives.gov/filescui20161206-cui-marking-handbook-		Υ	Y	
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 both internal and external to the organizational incident response capability.  3.6.3 Test the organizational incident response capability.  3.7 MAINTENANCE  3.7.1 Perform maintenance on organizational systems.  3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.  3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.  3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.  3.7.5 Require multifactor authentication to establish nonlocal maintenance essions at external network connections and terminate such connections when nonlocal maintenance is complete.  3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.  3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.  N Y We understand we should label rooms and machines according to https://www.archives.go/filescui/20161206-cui-marking-handbook-	·			
a permanent password.  3.5.10 Store and transmit only cryptographically-protected passwords.  Y Y Y  3.5.11 Obscure feedback of authentication information.  Y Y Y  3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.  3.6.2 Track, document, and report incidents to designated officials andor authorities both internal and external to the organization.  3.6.3 Test the organizational incident response capability.  3.7.4 MAINTENANCE  3.7.1 Perform maintenance on organizational systems.  3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.  3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.  3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.  3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions with a external network connections and terminate such connections when nonlocal maintenance is complete.  3.6.8 Spervise the maintenance activities of maintenance personnel without required access authorization.  3.8 MEDIA PROTECTION  3.8 MEDIA PROTECTION  3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.  N Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-				
3.5.10 Store and transmit only cryptographically-protected passwords. 3.5.11 Obscure feedback of authentication information. 3.6 INCIDENT RESPONSE 3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. 3.6.2 Track, document, and report incidents to designated officials andor authorities both internal and external to the organization. 3.6.3 Test the organizational incident response capability. 3.7.1 Perform maintenance on organizational systems. 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media to authorized users. 3.8.4 Mark media with necessary CUI markings and distribution limitations. N Y We understand we should label rooms and machines acording to https://www.archives.gov/filescui/20161206-cui-marking-handbook-		Υ	Y	
3.5.11 Obscure feedback of authentication information.  3.6 INCIDENT RESPONSE 3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. 3.6.2 Track, document, and report incidents to designated officials andor authorities both internal and external to the organization. 3.6.3 Test the organizational incident response capability. 3.7.4 Test the organizational incident response capability. 3.7.1 Perform maintenance on organizational systems. 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8.4 Diagnostic and test programs for mailicious code before the media access authorization. 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media to authorized users. 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-				
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 both internal and external to the organization. 3.6.3 Test the organizational incident response capability. 3.7.1 Perform amintenance on organizational systems. 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitze or destroy system media containing CUI before disposal or release for 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.go/filescui20161206-cui-marking-handbook-				
3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.  3.6.2 Track, document, and report incidents to designated officials andor authorities both internal and external to the organization. 3.6.3 Test the organizational incident response capability. 3.7 MAINTENANCE 3.7.1 Perform maintenance on organizational systems. 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media to authorized users. 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-		Υ	Υ	
that includes preparation, detection, analysis, containment, recovery, and user response activities.  3.6.2 Track, document, and report incidents to designated officials andor authorities both internal and external to the organization.  3.6.2 Track, document, and report incidents to designated officials andor authorities both internal and external to the organization.  3.6.2 Track, document, and report incidents to designated officials andor authorities both internal and external to the organization.  3.7.3 Erst the organizational incident response capability.  N Y  3.7.4 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.  3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.  3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.  3.7.5 Require multifactor authentication to establish nonlocal maintenance is complete.  3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.  3.8 MEDIA PROTECTION  3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  N Y  We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-				
sponse activities.  3.6.2 Track, document, and report incidents to designated officials andor authorities both internal and external to the organization.  3.6.3 Test the organizational incident response capability.  3.7 Maintenance  3.7.1 Perform maintenance on organizational systems.  3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.  3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.  3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.  3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.  3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.  3.8 MEDIA PROTECTION  3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  N Y  We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-		Υ	Y	,
3.6.2 Track, document, and report incidents to designated officials andor authorities both internal and external to the organization. 3.6.3 Test the organizational incident response capability. 3.7 MAINTENANCE 3.7.1 Perform maintenance on organizational systems. 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. N Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-	that includes preparation, detection, analysis, containment, recovery, and user re-			contract to look over logs etc. to note when we are hit.
both internal and external to the organization.  3.6.3 Test the organizational incident response capability.  N Y  3.7 MAINTENANCE  3.7.1 Perform maintenance on organizational systems.  Y Y  3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.  3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.  3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.  3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.  3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.  3.8 MEDIA PROTECTION  3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  N Y  We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-	•			
3.6.3 Test the organizational incident response capability. 3.7 MAINTENANCE 3.7.1 Perform maintenance on organizational systems. 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. N Y Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-		Υ	Y	
3.7 MAINTENANCE 3.7.1 Perform maintenance on organizational systems.  3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users.  N Y Y We understand we shoull label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-				
3.7.1 Perform maintenance on organizational systems. 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users.  3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.  N Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-		N	Y	
3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users.  N Y Sunderstand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-	3.7 MAINTENANCE			
conduct system maintenance.  3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.  3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.  3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.  3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.  3.8 MEDIA PROTECTION  3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.  3.8.4 Mark media with necessary CUI markings and distribution limitations.  N Y We understand we shoudl label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-				
3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.  N Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-		Υ	Y	
3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.  3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.  3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.  3.8 MEDIA PROTECTION  3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.  3.8.4 Mark media with necessary CUI markings and distribution limitations.  N Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-				
the media are used in organizational systems.  3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.  3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.  3.8 MEDIA PROTECTION  3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.  3.8.4 Mark media with necessary CUI markings and distribution limitations.  N Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-				
3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.  3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.  3.8 MEDIA PROTECTION  3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.  3.8.4 Mark media with necessary CUI markings and distribution limitations.  N Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-		Υ	Y	
via external network connections and terminate such connections when nonlocal maintenance is complete.  3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.  3.8 MEDIA PROTECTION  3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.  3.8.4 Mark media with necessary CUI markings and distribution limitations.  N Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-				
maintenance is complete.  3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.  3.8 MEDIA PROTECTION  3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.  3.8.4 Mark media with necessary CUI markings and distribution limitations.  N Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-	·		Y	Cristian Richard
3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.  3.8 MEDIA PROTECTION  3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.  3.8.4 Mark media with necessary CUI markings and distribution limitations.  N Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-				
quired access authorization.  3.8 MEDIA PROTECTION  3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.  3.8.4 Mark media with necessary CUI markings and distribution limitations.  N Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-	·			
3.8 MEDIA PROTECTION  3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.  3.8.4 Mark media with necessary CUI markings and distribution limitations.  N Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-		Υ	Y	
3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.  3.8.2 Limit access to CUI on system media to authorized users.  3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.  3.8.4 Mark media with necessary CUI markings and distribution limitations.  N Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-	·			
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 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-				
3.8.2 Limit access to CUI on system media to authorized users.  N Y  3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.  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-		N	Y	
3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.  3.8.4 Mark media with necessary CUI markings and distribution limitations.  N Y We understand we should label rooms and machines acording to https://www.archives.govfilescui20161206-cui-marking-handbook-	<u> </u>			
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-				
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-	3.8.3 Sanitize or destroy system media containing CUI before disposal or release for	Υ	Υ	
to https://www.archives.govfilescui20161206-cui-marking-handbook-				
	3.8.4 Mark media with necessary CUI markings and distribution limitations.	N	Y	_
v1-1.pdf				
				V1-1.pat



3.8.5 Control access to media containing CUI and maintain accountability for media	
during transport outside of controlled areas.	
3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI	
stored on digital media during transport unless otherwise protected by alternative	
physical safeguards.	
3.8.7 Control the use of removable media on system components.	
3.8.8 Prohibit the use of portable storage devices when such devices have no identi-	
fiable owner.	
3.8.9 Protect the confidentiality of backup CUI at storage locations.	
3.9 PERSONNEL SECURITY	
3.9.1 Screen individuals prior to authorizing access to organizational systems contain-	
ing CUI.	
3.9.2 Ensure that organizational systems containing CUI are protected during and af-	
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	
operating environments to authorized individuals.	
3.10.2 Protect and monitor the physical facility and support infrastructure for organi-	
zational systems.	
3.10.3 Escort visitors and monitor visitor activity.	
3.10.4 Maintain audit logs of physical access.	
3.10.5 Control and manage physical access devices.	
0 1 7	
3.10.6 Enforce safeguarding measures for CUI at alternate work sites.	
3.11 RISK ASSESSMENT	
3.11.1 Periodically assess the risk to organizational operations (including mission,	
functions, image, or reputation), organizational assets, and individuals, resulting from	
the operation of organizational systems and the associated processing, storage, or	
transmission of CUI.	
3.11.2 Scan for vulnerabilities in organizational systems and applications periodically	
and when new vulnerabilities affecting those systems and applications are identified.	
3.12 SECURITY ASSESSMENT	
3.12.1 Periodically assess the security controls in organizational systems to determine	
if the controls are effective in their application.	
3.12.2 Develop and implement plans of action designed to correct deficiencies and	
reduce or eliminate vulnerabilities in organizational systems.	
3.12.3 Monitor security controls on an ongoing basis to ensure the continued effec-	
tiveness of the controls.	
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 connections with a reprinting a system and communicating via some other connection to	
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	Y	Currently we have no mobile code
3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.			
3.13.15 Protect the authenticity of communications sessions.			
3.13.16 Protect the confidentiality of CUI at rest.	N	Y	
3.14 SYSTEM AND INFORMATION INTEGRITY			
3.14.1 Identify, report, and correct system flaws in a timely manner.	Υ	Y	
3.14.2 Provide protection from malicious code at designated locations within organizational systems.	N	N	
3.14.3 Monitor system security alerts and advisories and take action in response.	Υ	Y	
3.14.4 Update malicious code protection mechanisms when new releases are available.	Y	Y	
3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	Y	Y	
3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Y	Y	
Total requirements		108	
Total Rubin Intends to comply with		74	
Total Rubin Complies with in 2021		48	

#### **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



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