

Vera C. Rubin Observatory Data Management

CUI Rubin Observatory Data Security Standards Response

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

DMTN-199

Latest Revision: 2021-07-23





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

3 Response to the requirements

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

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

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

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.

¹{confidentiality, availability, integrity}



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 Refhres 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

We feel 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 2 . 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.

Decription	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 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 Vettign System is all FTE cost - apart from unknown hardware at LLNL.

Decription	Cost	Count	Total
FTE per year	\$500,000.00	2.5	\$1,250,000
Misison years		10	\$12,500,000
Pre operations years		3	\$3,750,000

²https://min.io/product/enterprise-object-storage-encryption



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	Intended	Note
	Status	Compli-	
		ance	
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	



out collusion. 3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts. 3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions. 3.1.9 Provide privacy and security notices consistent with applicable CUI rules. 3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. 3.1.11 Terminate (automatically) a user sessions. 3.1.12 Monitor and control remote access sessions. 3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. 3.1.14 Route remote access via managed access control points. 3.1.15 Authorize remote execution of mobile devices and mobile computing platforms. 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 1.10 In the sense there is no open wifi, and on the summit devices must be registered. 3.1.19 Encrypt CUI on mobile devices - in the case where an image may	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
and privilegid accounts. 31.1 Vernoem, roots when accessing nonlecurity functions. 31.2 Frence non-privilegid duscounts or roles when accessing nonlecurity functions. 31.3 Frence non-privilegid duscrises from executing privilegid functions and capture free execution of a with functions in audit growth incrines in audit growth functions in audit growth functions. 31.19 Frence when functions in audit growth functions in audit growth functions in audit growth functions in audit growth functions. 31.15 Monitor and control remote access sessions. 31.15 English crowth functions in audit growth function in audit growth function in audit growth function in audit growth function in a control remote access sessions. 31.15 Monitor and control remote access sessions. 31.16 Monitor and control remote access sessions. 31.17 Monitor and control remote access sessions. 31.18 Monitor and control remote access sessions. 31.19 Monitor and control remote access sessions. 31.10 Monito	·	IN	'	
31.6 User non privileged accounts or roles when accessing nonsecurity functions and capture the execution of such functions in audit logs. 31.7 Prevent nonprivileged users from executing privileged functions and capture the execution of such functions in audit logs. 31.8 Limit impraced buildings attempts. N V I I don't before we do this new but we car, this is not done for solor hosts or network equipment. Web Services such as low, foreign for the such as a such as lower than the such as lower than the such as a such as lower than the such as lower		N	Y	Targeted sudo rules are needed for common operations
3.1.2 Premote protection provideged super consumers and capture the execution of such furthers in audit gravity and security protection strategy and security protection and applicable CULINDE. 3.1.5 Provide privary and security protects consistent with applicable CULINDE. 3.1.5 Provide privary and security protects consistent with applicable CULINDE. 3.1.5 Provide privary and security protects consistent with applicable CULINDE. 3.1.5 Provide privary and security protects consistent with applicable CULINDE. 3.1.5 Provide privary and security protects consistent with applicable CULINDE. 3.1.5 Provide privary and security protects consistent with applicable CULINDE. 3.1.6 Provide privary and security protects access sections. 3.1.1 Provides temperature section shall deplay to prevent access and viewing of view and control remote access sections. 3.1.1 Provides temperature section shall be confidentially of remote access sections. 3.1.1 Monitor and control remote access sessions. 3.1.1 Provides temperature section of monitors of the confidentially of remote access sessions. 3.1.1 Provides temperature section of monitors of the confidentially of remote access to an applicable community of the confidentially of remote access to a managed access soft and applicable community of the confidentially of remote access to a managed access to a		V	V	
the execution of such functions in audit logs. 31.8 limit insurvicesful liging attempts. N Y I don't believe we do this now but we can; this is not done for soll or hosts or network equipment. Web Services such as low, forerant just comment. Web Services such as low, forerant just comment in the summer such such as low, and in the summer such as low to the summer such as low, and in the summer such as low to the summer such such as low to the summer such as low		'		Cristian Dishard does this include SLIDO 2 Does this mean DOSIV
hosts or network equipment. Web Services such as love, foreman fips cronsic, milation, etc., methods privacy and security notices consistent with applicable CUI rules. 3.1.9 Frouded privacy and security notices consistent with applicable CUI rules. 3.1.10 Use session lock with pattern-finding displays to prevent access and wewing of data after a period of inactivity. 4.1.13 Emmission control of inactivity is a session after a defined condition. 5.1.14 Internative and control remote access sessions. 5.1.15 Emmission control access sessions. 7.1.15 Employ cryptographite mechanisms to protect the confidentiality of remote acc. 7.1.15 Employ cryptographite mechanisms to protect the confidentiality of remote acc. 7.1.15 Employ cryptographite mechanisms to protect the confidentiality of remote acc. 7.1.15 Employ cryptographite mechanisms to protect the confidentiality of remote acc. 7.1.15 Employ cryptographite mechanisms to protect the confidentiality of remote acc. 8.1.16 Employ cryptographite mechanisms to protect the confidentiality of remote acc. 9.1.17 Employ cryptographite mechanisms to protect the confidentiality of remote acc. 10.1.16 Employ cryptographite mechanisms to protect the confidentiality of remote acc. 10.1.16 Employ cryptographite mechanisms to protect the confidentiality of remote acc. 10.1.16 Employ cryptographite mechanisms to protect the confidentiality of remote acc. 10.1.16 Employ cryptographite mechanisms to protect the confidentiality of remote acc. 10.1.16 Employ cryptographite mechanisms to protect the confidentiality of remote acc. 10.1.16 Employ cryptographite mechanisms to protect the confidentiality of remote acc. 10.1.16 Employers access using a mechanisms to protect the confidentiality of remote acc. 10.1.16 Employers access using a mechanisms to protect the confidentiality of remote access the confidentiality of remote access the confidential transport access to the confidential transport access the confidential transport access to the confidential transport ac	the execution of such functions in audit logs.		Y	
is a consider, mulabole, exec, may yeed rate limiting 3.1.0 foreoide privacy and security notices consistent with applicable CUI rules. 3.1.0 Use session lock with pattern-liding displays to prevent access and wewing of V V This is our policy. 3.1.11 Terminate (automatically) a user session after a defined condition. 3.1.11 Terminate (automatically) a user session after a defined condition. 3.1.12 Imminor and control remote access sessions. 3.1.13 Primply cyptographic mechanisms to protect the confidentially of remote ac V V PN is in user a few do this now. 3.1.14 Surplicy cyptographic mechanisms to protect the confidentially of remote ac V PN is in user a few do this now. 3.1.15 Imply cyptographic mechanisms to protect the confidentially of remote ac V PN is in user a few do this now. 3.1.16 Surplicy cyptographic mechanisms to protect the confidentially of remote ac V PN is in user a few do this now. 3.1.16 Surplicy cyptographic mechanisms to protect the confidentially of remote ac V PN is in user a few do this now. 3.1.16 Surplicy cyptographic mechanisms to protect the confidentially of remote ac V PN is in user a few do this now. 3.1.16 Surplicy cyptographic mechanisms to protect the confidentially of remote ac V PN is in user a few do this now. 3.1.16 Surplicy cyptographic mechanisms to protect the confidentially of remote ac V PN is in user a few do this now. 3.1.16 Surplicy cyptographic mechanisms to protect the confidentially of remote access to the surplication of the confidential to the confidential of the confidential to the confidential to the confidential to confidentially of remote access to the surplication of the confidential to confidentially of remote access to the confidential to confidentially of the confidentially of the confidentially of the confidentially of the con	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
3.1.9 Eversion for execution of privileged community and executive previous executions of privileged community and executive previous executions and executive previous executions and executive previous executions and executive previous executions are previous executions. 3.1.13 Empiricy cryptographic mechanisms to protect the confidentiality of remote access sessions. 3.1.13 Empiricy cryptographic mechanisms to protect the confidentiality of remote access sessions. 3.1.14 Empiricy cryptographic mechanisms to protect the confidentiality of remote access sessions. 3.1.15 Empiricy cryptographic mechanisms to protect the confidentiality of remote access sessions. 3.1.16 Empiricy cryptographic mechanisms to protect the confidentiality of remote access sessions. 3.1.16 Engine remote access six amanaged access control points. 3.1.16 Engine remote access six amanaged access control points. 3.1.16 Engine remote access six amanaged access control points. 3.1.16 Engine remote access six amanaged access control points. 3.1.16 Engine remote access six amanaged access control points. 3.1.16 Engine remote access six amanaged access control points. 3.1.16 Engine remote access six amanaged access control points. 3.1.16 Engine remote access six amanaged access control points. 3.1.16 Engine remote access six amanaged access control points. 3.1.16 Engine remote access six amanaged access control points. 3.1.16 Engine remote access six amanaged access control points. 3.1.16 Engine remote access six amanaged access control points. 3.1.16 Engine remote access six amanaged access control points. 3.1.16 Engine remote access six amanaged access control points. 3.1.17 Engine remote access six amanaged access control points. 3.1.18 Engine remote access six amanaged access six amanaged access control points. 3.1.18 Engine remote access six amanaged access acc				hosts or network equipment. Web Services such as love, foreman,
3.1.15 Enrops CLU in mobile devices and mobile computing platforms.23 3.1.19 Force your CLU in mobile devices and mobile computing platforms.23 3.1.20 Verify and controllimit connections to and use of external systems. 3.1.21 Limit use of portable storage devices on external systems. 3.1.22 Limit use of portable storage devices on external systems. 3.1.22 Limit use of portable storage devices on external systems. 3.1.23 Limit use of portable storage devices on external systems. 3.1.23 Limit use of portable storage devices on external systems. 3.1.24 Limit use of portable storage devices on external systems. 3.1.25 Limit use of portable storage devices on external systems. 3.1.26 Limit use of portable storage devices on external systems. 3.1.27 Limit use of portable storage devices on external systems. 3.1.28 Limit use of portable storage devices on external systems. 3.1.29 Limit use of portable storage devices on external systems. 3.1.21 Limit use of portable storage devices on external systems. 3.1.22 Limit use of portable storage devices on external systems. 3.1.23 Limit use of portable storage devices on external systems. 3.1.24 Limit use of portable storage devices on external systems. 3.1.25 Limit use of portable storage devices on external systems. 3.26 Limit use of portable storage devices on external systems. 3.27 Limit use of portable storage devices on external systems. 3.28 Limit use of portable storage devices on external systems. 3.29 Limit use of portable storage devices on external systems. 3.20 Limit use of portable storage devices on external systems. 3.21 Limit use of portable storage devices on external systems. 3.22 Limit use of portable storage devices on external systems. 3.23 Limit use of portable storage devices on external systems. 3.24 Alkaric than the external system sample portable devices and external system sample portable devices and external systems administrators, and users of organizational systems administratory and controllimit connections to an user and external system such				ipa console, nublado, etc. may need rate limiting
data after a period of inactivity. 31.17 Erminate (controllation) as user assistion after a defined condition. N Y shadows are generally not limited on hosts; some network equipment has timenate set, nublado has a session limit for notebook? 31.18 Monitor and control remote access sessions. N Y Cristian not sure if we do this now. 31.18 Definition of the service of the confidentiality of remote access sessions. N Y V PVN is in use consistent and access control points. 31.18 Control control of privileged commands and remote access to security releast information. 31.16 Authorition wereless access prior to allowing such connections. 31.17 Princet wereless access prior to allowing such connections. 31.18 Control connection of mobile devices and mobile computing platforms. 31.19 Encrypt CUI on mobile devices and mobile computing platforms. 31.19 Encrypt CUI on mobile devices and mobile computing platforms. 31.20 Verify and controllimit connections to and use of external systems. 31.20 Verify and controllimit connections to and use of external systems. 31.21 Intrins use of portable storage devices on external systems. 31.22 Control CUI portable storage devices on external systems. 31.22 Control CUI portable storage devices on external systems. 31.22 Control CUI portable storage devices on external systems. 31.22 Control CUI portable storage devices on external systems. 31.24 Intrins use of portable storage devices on external systems. 31.24 Ensure that personnel are trained to carry out their assigned information excursive free for inspirate and exercise of mobile plates of exercise systems. 31.24 Provides duties and responsibilities. 32.24 Provides duties and resources and inspiration and exercise of exercise for device operations and the propriet of individual system users can be uniquely traced to the executive of the exercise for device operations and the exercise of insider threat. 33.24 Provides duties and resources and provide general exercises for device operations and the exercise of	3.1.9 Provide privacy and security notices consistent with applicable CUI rules.	N	Y	Check login notices etc.
3.1.11 Monitor and control remote access sessions. 3.1.2 Monitor and control remote access sessions. 3.1.2 Monitor and control remote access sessions. 3.1.3 Employ regographic mechanisms or protect the confidentiality of remote access sessions. 3.1.4 Router emote access via managed access control points. 3.1.5 Authorities remote access via managed access control points. 3.1.5 Authorities remote access via managed access control points. 3.1.6 Authorities remote access via managed access control points. 3.1.6 Authorities remote access via managed access control points. 3.1.6 Authorities remote access via managed access control points. 3.1.6 Authorities remote access via managed access control comments and remote access to security-relevant information. 3.1.6 Authorities wireless access using authoritication and encryption. 3.1.6 Protect wireless access using authoritication and encryption. 3.1.8 Protect wireless access using authoritication and encryption. 3.1.9 Encrypt CUI on mobile devices and mobile computing platforms 23 3.1.9 Encrypt CUI on mobile devices and mobile computing platforms 23 3.1.9 Encrypt CUI on mobile devices and mobile computing platforms 23 3.1.1 Limit use of portable storage devices on external systems. 3.1.2 Virily and controllimit connections to and use of esternal systems. 3.1.2 Limit use of portable storage devices on external systems. 3.1.2 Limit use of portable storage devices on external systems. 3.1.2 Virily and controllimit connections to and use of esternal systems. 3.1.2 Virily and controllimit connections to and use of esternal systems. 3.1.2 Virily and controllimit connections to and use of esternal systems. 3.1.2 Virily and controllimit connections to and use of esternal systems. 3.1.2 Virily and controllimit connections to and use of esternal systems. 3.1.3 Limit use of portable storage devices on external systems. 3.1.4 Virily and controllimit connections to and use of esternal systems. 3.1.5 Virily and controllimit connections to an use of esternal systems. 3.1.4 Virily and	1 0 1 7 1	Y	Y	This is our policy.
ment has timenuts set, nublado has a session limit for notebooks? 3.1.12 Monitor and control remote access sessions. 3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. 3.1.14 Boats remote access via managed access control points. 3.1.15 Authorize with managed access control points. 3.1.16 Authorize with execution of privileged commands and remote access to security relevant information. 3.1.16 Authorize with execution of privileged commands and remote access to y v security relevant information. 3.1.16 Authorize with exess access prior to allowing such connections. 3.1.17 Protect wireless access prior to allowing such connections. 3.1.18 Charolize remote execution of privileged commands and remote access to y v security relevant information. 3.1.18 Charolize remotes access prior to allowing such connections. 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms. 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms. 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms. 3.1.20 Verify and controllimit connections to and use of external systems. 3.1.20 Verify and controllimit connections to and use of external systems. 3.1.21 Limit use of portable storage devices on external systems. 3.1.21 Limit use of portable storage devices on external systems. 3.1.22 Charolic Clin control of protections on publicly accessible systems. 4.22 Avance of the security risks associated with their activities and of the applicable policies and publicly accessible systems. 4.23 Avance of the security risks associated with their activities and of the applicable policies standards, and procedures related to the security of those systems. 4.24 Provide security avancers to trining on recognizing and reporting to those systems. 5.25 Provide security waverness training on recognizing and reporting to their activities and of the employable provides and of the activity. 5.26 Provide security avancers to raining on recognizing and reporting to this externa			.,	
3.1.15 Authorise mechanisms to protect the confidentiality of remote access seasons. 3.1.16 Authorise member excess of managed access control points. 3.1.16 Authorise member excess to privileged commands and remote access to security-relevant information. 3.1.16 Authorise member excess to privileged commands and remote access to security-relevant information. 3.1.16 Authorise members access prior to allowing such connections. 3.1.17 Protect wireless access using authentication and encyption. 3.1.18 Control connection of mobile devices. 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23 3.1.21 Limit use of portable storage devices on access the section of mobile devices in the case where an image may exist on say commissioning team laptop we will have disk encryptor enabled. 3.1.22 Limit use of portable storage devices on external systems. 3.1.23 Avanisms Authorise and expension of the control network. 3.1.24 Limit use of portable storage devices on external systems. 3.1.25 Control CUI posted or processed on publicly accessible systems. 3.1.26 Avanisms Authorise and expensional systems. 3.1.27 Limit use of portable storage devices on external systems. 3.1.28 Avanisms Authorise and expensional systems. 3.1.29 Avanisms Authorise and expensional systems. 3.20 Ensure that personnel are trained to carry out their assigned information security-related duties and responsabilities. 3.2.3 Provide security wavereness training on recognizing and reporting potential in dictators of misdetic and responsabilities. 3.2.3 Fourities and expensional systems. 3.3 Alorest the actions of individual system users can be uniquely traced to the extent needed to enable the monitoring, analysis, increases and synchronized systems activity. 3.3.4 Refer the devices and responsability that conductions of unlawful, unauraborized associations of unlawful unauraborized systems. 3.3.4 R	3.1.11 Terminate (automatically) a user session after a defined condition.	N	Y	
sess sessions. 3.1.5 All Authorizes remote access via managed access control points. 3.1.5 All Authorizes remote access via managed access control points. 3.1.5 Authorizes remote access via managed access control points. 3.1.5 Authorizes remote access via managed access control points. 3.1.5 Authorizes remote access via managed access control points. 3.1.6 Authorizes remote access via managed access control points. 3.1.6 Authorizes remote access via managed access control points. 3.1.6 Authorizes remote access via managed access control points. 3.1.6 Authorizes remote access via managed access to remove the control common to manage via the control common to manage via the control common to more control control common to manage via the control common to manage via the control common to manage via the control common to commissioning terms labored with the access to the control nework. 3.1.2 Overfly and controllimit connections to and use of external systems. 3.1.2 Unit use of portale storage devices on external systems. 3.1.2 Control Culp posted or processed on publicly accessible systems. 3.1.2 Control Culp posted or processed on publicly accessible systems. 3.1.2 Control Culp posted or processed on publicly accessible systems. 3.1.2 All removes the managers, systems administrators, and users of organizational systems. 3.1.2 Fainer that practices and the post Cull on publicly accessible systems. 3.1.2 Fainer that practices and of the security of those systems. 3.1.2 Fainer that practices and of the security of those systems. 3.1.2 Fainer that practices and of the security of those systems. 3.1.2 Fainer that practices and of the security of those systems. 3.1.2 Fainer that practices and of the security of those systems. 3.1.2 Fainer that practices and of the security of those systems. 3.1.3 Fainer that the actions of uniforally unauthorized systems. 3.1.4 Fainer than and the post Cull on publicly accessible systems. 3.1.5 Fainer that practices and of the security of those systems. 3.1.6 Fainer than a fainer syst	3.1.12 Monitor and control remote access sessions.	N	Y	Cristian - not sure if we do this now
3.1.14 Suthorise remote access to privileged commands and remote access to y y y security-relevant information. 3.1.15 Authorise remote secution of privileged commands and remote access to y y y y y y y y y y y y y y y y y y	3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Υ	Y	VPN is in use
3.1.15 Authorize remote execution of privileged commands and remote access to V V Security-relevant information. 3.1.16 Authorize wireless access using authentication and encryption. 3.1.16 Control connection of mobile devices. 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23 3.1.10 Encrypt CUI on mobile devices and mobile computing platforms.23 3.1.20 Verify and controllimit connections to and use of external systems. 3.1.20 Verify and controllimit connections to and use of external systems. 3.1.21 Limit use of portable storage devices on external systems. 3.1.22 Control (Limit use of portable storage devices on external systems. 3.1.22 Control (Limit use of portable storage devices on external systems. 3.1.23 Enrollimit use of portable storage devices on external systems. 3.1.24 Authorities with the storage devices on external systems. 3.1.24 Control (Limit use of portable storage devices on external systems. 3.1.24 Control (Limit use of portable storage devices on external systems. 3.1.24 Control (Limit use of portable storage devices on external systems. 3.1.24 Control (Limit use of portable storage devices on external systems. 3.1.24 Control (Limit use of portable storage devices on external systems. 3.25 Enrollimit that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the application of the systems administrators, and users of organizational systems. 3.25 Enrollimit has personnel are trained to carry out their assigned information security-valued duties and responsibilities. 3.25 Enrollimit has personnel are trained to carry out their assigned information security-valued duties and responsibilities. 3.26 Enrollimit has accorded to the extent needed to enable the monitoring, analysis, investigation, and reporting for information of more devices and training and reporting processes for investigation in a supplication of		N	Y	Bastion nodes – LHN is an open back door with no ACLs
security-relevant information. 3.1.16 Authorite wireless access prior to allowing such connections. 3.1.17 Protect wireless access using authentication and encryption. 3.1.18 Control connection of mobile devices. 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23 3.1.20 Verify and controllimit connections to and use of external systems. 3.1.20 Verify and controllimit connections to and use of external systems. 3.1.21 Limit use of portable storage devices on external systems. 3.1.21 Limit use of portable storage devices on external systems. 3.1.22 Control CUI postad or processed on publicly accessible systems. 3.1.22 Flourer than maragers, systems administrators, and users of organizational systems. 3.1.22 Flourer than transagers, systems administrators, and users of organizational systems. 3.23 Provide security awareness training on recognizing and reporting potential indicators of insider threat. 3.3.24 Flourer that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.3.24 Flourer that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.3.24 Flourer that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.3.24 Flourer that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.3.2 Flourer that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.3.2 Flourer that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.3.2 Flourer that personnel are trained to carry out their assigned information and carry out their assigned information and personnel are trained to the security of those systems. 4 Y 4 We would like to do more here like capture flag exercises for devel				
3.1.16 Control connection of mobile devices and mobile computing platforms.23 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23 3.1.20 Verify and controllimit connections to and use of external systems. 3.1.20 Verify and controllimit connections to and use of external systems. 3.1.20 Verify and controllimit connections to and use of external systems. 3.1.21 Limit use of portable storage devices on external systems. 3.1.22 Limit use of portable storage devices on external systems. 3.1.22 Control CUI posted or processed on publicly accessible systems. 3.1.22 Control CUI posted or processed on publicly accessible systems. 3.1.22 Control CUI posted or processed on publicly accessible systems. 3.22 AWARENESS AND TRAINING 3.2.1 Ensure that managers, systems administrators, and users of organizational systems. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duises and responsibilities. 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of inside its and responsibilities. 3.2.3 Ensure that the actions of individual system users can be uniquely traced to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.4 Ensure that the actions of individual system users can be uniquely traced to the monitoring analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.4 Forwise and carry out and the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.4 Forwise and read in system audit logging process failure. 3.3.2 Forwise that the actions of individual system users can be uniquely traced to the extent needed to enable the monitoring, analysis, investigation and report generate timestamps for audit reco	· · · · · · · · · · · · · · · · · · ·	i i		
3.1.17 Entropyt CUI on mobile devices and mobile computing platforms 23 3.1.18 Control connection of mobile devices and mobile computing platforms 23 3.1.18 Control connection of mobile devices and mobile computing platforms 23 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms 23 3.1.20 Varify and controllimit connections to and use of external systems. 3.1.20 Varify and controllimit connections to and use of external systems. 3.1.20 Varify and controllimit connections to and use of external systems. 3.1.20 Varify and controllimit connections to and use of external systems. 3.1.20 Varify and controllimit connections to and use of external systems. 3.1.21 Limit use of portable storage devices on external systems. 3.1.21 Limit use of portable storage devices on external systems. 3.1.21 Control CUI posted or processed on publicly accessible systems. 3.2.24 National managers, systems administrators, and users of organizational systems are made aware of the security risks associated with the extensive and of the security risks associated with their activities and of the splicible policies, standards, and reportabilities. 3.2.2 Provide sourity awareness training on recognizing and reporting potential involved tuties and responsibilities. 3.2.2 Provide sourity awareness training on recognizing and reporting potential involved tuties and retain system auditiogs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or mustuhorized system activity. 3.2.2 Finance that the actions of individual system users can be uniquely traced to the monitoring, analysis, investigation, and reporting processes for investigation and reporting processes for investigation and response to indications of unlawful unauthorized systems. P Y We may look for a third party contract for this. 3.2 Provide a system capability that compares and synthronizes internal system. 3.3 Provide a pytem capability that compares and synthronizes internal system. 4.1.2 Provides a pytem ca	· · · · · · · · · · · · · · · · · · ·	V	- V	All device attaching in Chile need to be registered by Mac address
3.1.18 Control connection of mobile devices. Y V In the sease there is no open will, and on the summit devices mus be registered. 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23 Y V CUI will not exist on mobile devices in the case where an image may exist on say commissioning team laptop we will have disk encryptor enabled. 3.1.20 Verify and controllimit connections to and use of external systems. Y V This implies vetting of devices that connect to the control netword we use man address for laptops and personal mobile phones car not connect to the control netword. 3.1.21 Limit use of portable storage devices on external systems. N Y CristianRichan SAN Trainings 3.1.22 Enter that managers, systems administrators, and use of organizational systems. A Was AND Training SAN				All devies attaching in chile need to be registered by wae address.
be registered. 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms 23 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms 23 3.1.20 Verify and controllimit connections to and use of external systems. 3.1.20 Verify and controllimit connections to and use of external systems. 3.1.20 Verify and controllimit connections to and use of external systems. 3.1.21 Limit use of portable storage devices on external systems. 3.1.22 Control CUI posted or processed on publicly accessible systems. 3.1.22 Control CUI posted or processed on publicly accessible systems. 3.2.2 MARKNESS AND TRAINING 3.2.2 Finsure that manager, systems administrators, and users of organizational systems. 4. Y 4. We do not intend to post CUI on publicly accessible systems. 5. Y 5. We do not intend to post CUI on publicly accessible systems. 6. Y 7. We do not intend to post CUI on publicly accessible systems. 8. A 8. Y 8. Y 8. We would like to do more here like capture flag exercises for devel deuters of inside the train system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Finsure that the actions of individual system users can be uniquely traced to the source of the activity of of the activi				In the case there is no ones wife and on the summit devices must
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. V V This implies vetting of devices that connect to the control network we use max address for laptops and personal mobile phones car not connect to the control network. 3.1.21 Limit use of portable storage devices on external systems. N V Cristianikchard - impliesn no USB drives etc enabled 3.1.22 Control (CUI) posted or processed on publicly accessible systems. N V We do not intend to post CUI on publicly accessible systems. 2.2 Flasure that manager, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policide, standards, and procedures related to the security of those systems. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat. 3.3.4 Lorent and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.3 Alvaire the exections of individual system users can be uniquely traced to these users, so they can be held accountable for their actions. N Y We may look for a third party contract for this. 3.3.4 Alvaire the vent of an audit logging grocess failure. N Y We may look for a third party contract for this. 3.3.5 Provide audit record review, analysis, and reporting processes for investigation and analysis and reporting. 3.3.6 Provide audit record review analysis, and reporting processes for investigation and analysis and reporting. 3.3.7 Provide a sudit information and				be registered.
a.1.20 Verify and controllimit connections to and use of external systems. V V This implies wetting of devices that connect to the control network we use mac address for laptops and personal mobile phones car not connect to the control network we use mac address for laptops and personal mobile phones car not connect to the control network we use mac address for laptops and personal mobile phones car not connect to the control network we use mac address for laptops and personal mobile phones car not connect to the control network. 3.1.20 Control CUI posted or processed on publicly accessible systems. 3.1.22 Control CUI posted or processed on publicly accessible systems. 3.2.2 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Provide security awareness training on recognizing and reporting potential involved duties and responsibilities. 3.3.4 NUDIT AND ACCOUNTABILITY 3.3.1 Croste and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to the monitoring, analysis, investigation, and reporting for inhawful or unauthorized system activity. 3.3.3 Provide audit record review, analysis, and reporting processes for investigation and response to individual system users can be uniquely traced to the security of their actions. P P Y We may look for a third party contract for this. 3.3.4 Alert in the went of an audit logging process failure. N Y We may look for a third party contract for this. 3.3.5 Protevide audit record review, analysis, and reporting processes for investigation and respo	3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23	Υ	Y	CUI will not exist on mobile devices - in the case where an image may
3.1.20 Verify and controllimit connections to and use of external systems. 3.1.21 Limit use of portable storage devices on external systems. 3.1.22 Control CUI posted or processed on publicly accessible systems. 3.2.2 Control CUI posted or processed on publicly accessible systems. 3.2.2 MARENESS AND TRAINING 3.2.1 Ensure that managers, systems administrators, and users of organizational systems. 3.2.2 Ensure that managers, systems administrators, and users of organizational systems. 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of inside threat. 3.3.4 Unit Annual Account Abstraction of the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.3 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Provide audit record review, analysis, and reporting processes for investigation analysis and responsibility that compares and synchronizes internal system decisions of unidarity that compares and synchronizes internal system decisions of unidarity that compares and synchronizes internal system close with an authoritative source to generate timestymps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, and all system closes with an authoritative source to generate timestymps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, and all system closed with an authoritative source to generate timestymps for audit records. 3.3.4 Protect audit information and audit logging functionality to a subset of privileged users. 3.4 Establish and enforce security config				exist on say commissioning team laptop we will have disk encryption enabled.
- we use max address for laptops and personal mobile phones car not connect to the control network. 3.1.21 Limit use of portable storage devices on external systems. 3.1.22 Control CUI posted or processed on publicly accessible systems. 3.2 AWARENESS AND TRAINING 3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat. 3.3 AUDIT AND ACCOUNTABILITY 3.3 LOTEARD ACCOUNTABILITY 3.3 LOTEARD ACCOUNTABILITY 3.3 Create and retain system audit logs and records to the extent needed to enable the monitoring analysis, investigation, and reporting for unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to the work of an audit logging process failure. N 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 Again shall look for third party contract for this and responses to indications of uniquely. unauthorized, suspicious, or unusual activity. 3.3.5 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.6 Provide audit record reduction and audit logging process for audit records. 3.3.8 Provide a system capability that compares and synchronizes internal system docks with an authoritative source to generate timestamps for audit records. 3.3.9 Provide audit information and audit logging tools from unauthorized access, yellow the expective system development life cycles. 3.3.1 Ensure that the actions of additions and inventories of organizational system (including hardware, software, firmware, and docu	3.1.20 Verify and controllimit connections to and use of external systems.	Υ	Y	
1.21 Limit use of portable storage devices on external systems. 1.21 Control CUI posted or processed on publicly accessible systems. 2.3.2 AWARENESS AND TRAINING 3.2.2 Control CUI posted or processed on publicly accessible systems. 2.4 Fasure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policities, standards, and procedures related to the security of those systems. 2.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of inside threat. 3.3 AUDIT AND ACCOUNTABILITY 3.3 Increate and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. P Y We may look for a third party contract for this. 3.3.4 Secondary dupdate logged events. P Y We may look for a third party contract for this. 3.3.5 Correlate a udit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.5 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Ensure that the actions of unlawful, unauthorized, suspicious, or unusual activity. 3.3.8 Provide a update logged events. 3.3.8 Provide a update logged events. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.3.4 Co				
3.122 Control CUI posted or processed on publicly accessible systems. 3.2 AWARENESS AND TRAINING. 3.2 Insure that managers, systems administrators, and users of organizational systems. 3.2 AWARENESS AND TRAINING. 3.2.1 Ensure that managers of the applicable policies, standards, and procedures related to the security of those systems. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat. 3.3 AUDIT AND ACCOUNTABILITY 3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.3 Review and update logged events. 3.3.4 ABOTT AND ACCOUNTABILITY 3.3.4 Forwide and understand to suppose to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.5 Correlate adult record review, analysis, and reporting processes for investigation and reporting. 3.3.6 Provide a system capability that compares and synchronizes internal system of work with an authoritative source to generate timestamps for audit records. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. Y We have CCBs and code change process in place which also cove				
3.12 Control CUI posted or processed on publicly accessible systems. 3.2 AWARENESS AND TRAINING 3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat. 3.3.4 DIDIT AND ACCOUNTABILITY 3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. N Y Again shall look for a third party contract for this. 3.3.5 Provide audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.1 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.1 Provide a system capability that compares and synchronizes internal system (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4 CONFIGURATION MANAGEMENT 3.4 Track, review, approve or disapprove, and log changes to organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	3.1.21 Limit use of nortable storage devices on external systems	N	- V	
3.2 AWARENESS AND TRAINING 3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat. 3.3.4 NDIPT AND ACCOUNTABILITY 3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. P				
3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Envoide security awareness training on recognizing and reporting potential indicators of insider threat. 3.3 AUDIT AND ACCOUNTABILITY 3.3.3 Loreate and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Provide audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Provide audit information and audit logging tools from unauthorized access, and 4 CONFIGINATION MANAGEMENT 3.4 CONFIGINATION MANAGEMENT 3.4 CONFIGINATION MANAGEMENT 3.4 I Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	<u> </u>	'	'	We do not intend to post cor on publicly accessible systems.
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 systems. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat. 3.3.4 DIT AND ACCOUNTABILITY 3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.5 Provide a udit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.7 Provide a udit record review, analysis, and reporting processes for investigation and years and system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Proved and information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Trock audit information and audit logging tools from unauthorized access, modification, and deletion. 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.		V	- V	
applicable policies, standards, and procedures related to the security of those systems. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Provide accurity awareness training on recognizing and reporting potential indicators of insider threat. 3.3.4 DIDT AND ACCOUNTABILITY 3.3.3 Loreat and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 It management of audit logging functionality to a subset of privileged users. 4 Y Y 4 We use mainly infrastructure as code approaches so the software is well tracked. It inventory all the hardware. 5 Y Y 5 We use mainly infrastructure as code approaches so the software is well tracked. It inventory all the hardware. 5 Y Y 5 We have CCBs and code change process in place which also covered to the process in place which also covered to the process in place which also covered to the process of the process in place which also covered to the process in place which also covered to the process of the process in place which also covered to the process in place which also covered to the process i		'	'	
tems. 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat. 3.3 AUDIT AND ACCOUNTABILITY 3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system docks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.1 Imit management of audit logging functionality to a subset of privileged users. 4 CONFIGURATION MANAGEMENT 4.4 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and entitain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. 3.4.2 Track, review, approve or disapprove, and log changes to organizational systems.	· ·			
3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. 3.2.3 Provide a system agability that compares and synchronizes internal system of such responsibilities. 3.3 AUDIT AND ACCOUNTABILITY 3.3 AUDIT AND ACCOUNTABILITY 3.3 AUDIT AND ACCOUNTABILITY 4.7 We would like to do more here like capture flag exercises for devel opers. 3.4 AUDIT AND ACCOUNTABILITY 3.3.2 Fixed and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Fixed and place logged events. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.5 Provide a unit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system odification, and deletion. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Imit management of audit logging functionality to a subset of privileged users. 4.7 Y 4.7 Y 4.8 We may look for a third party contract for this. 4.9 Again shall look for third party contract for this. 4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configurations settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational system.				
security-related duties and responsibilities. 3.2.3 Provide security wareness training on recognizing and reporting potential indicators of insider threat. 3.3 AUDIT AND ACCOUNTABILITY 3.3.1 Create and retatin system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Provide a dutin information and audit logging functionality to a subset of privileged users. 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configurations settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational system.		N	- V	
3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat. 3.3.4 DIT NAD ACCOUNTABILITY 3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.8 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.9 Frovide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.8 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. Y Y We use mainly infrastructure as code approaches so the software is well tracked. IT inventory all the hardware. We use mainly infrastructure as code approaches so the software is well tracked. IT inventory all the hardware.		IN .	'	
dicators of insider threat. 3.3 AUDIT AND ACCOUNTABILITY 3.3 AUDIT AND ACCOUNTABILITY 3.3 AUDIT AND ACCOUNTABILITY 3.3 I create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.4 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configurations settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. 4 Y We have CCBs and code change process in place which also covered to the process in place which also		V	- V	We would like to do more here like capture flag eversions for devel
3.3 AUDIT AND ACCOUNTABILITY 3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide a udit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system docks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 4.4 CORFIGURATION MANAGEMENT 3.4.1 Establish and aminatin baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.		'	'	· -
3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. Y We have CCBs and code change process in place which also covered as a process of the soft and covered and covered covered and covered covered and covered change process in place which also covered covered and covered change process in place which also covered covere				opers.
the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.4 CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.2 Increase of the actions of individual systems in a uniquely traced to the actions. Y Y We have CCBs and code change process in place which also covered to the actions.				
tem activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4 CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational sys-		, i	Y	
3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. Y Y We have CCBs and code change process in place which also covered to the province of the process in place which also covered to the province of the process in place which also covered to the process				
those users, so they can be held accountable for their actions. 3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. Y We have CCBs and code change process in place which also covered to the software in specific cycles.	· · · · · · · · · · · · · · · · · · ·	.,		
3.3.3 Review and update logged events. 3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. 9 Y We have CCBs and code change process in place which also covered to the maintain base contract for this. 9 Y We may look for third party contract for this. 9 Again shall look for third party contract for this. 9 Again shall look for third party contract for this. 9 Again shall look for third party contract for this. 9 Again shall look for third party contract for this. 9 Again shall look for third party contract for this. 9 Again shall look for third party contract for this. 9 Again shall look for third party contract for this. 9 Again shall look for third party contract for this. 9 Again shall look for third party contract for this. 9 Again shall look for third party contract for this. 9 Again shall look for third party contract for this.		Y	Y	
3.3.4 Alert in the event of an audit logging process failure. 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4. CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology and the products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. 3.4.2 Establish and enforce security configuration settings for information technology and the products employed in organizational systems.		D	- V	We may look for a third party contract for this
3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. 3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4 CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. N				We may look for a tillia 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. 3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4.1 CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. Y Y We have CCBs and code change process in place which also cover				Again shall look for third party contract for this
3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4 CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. Y Y We have CCBs and code change process in place which also covered to the control of the cont		IN .	Y	Again Shall look for third party contract for this
analysis and reporting. 3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4 CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. Y Y We have CCBs and code change process in place which also covered to the comparison of the process in place which also covered to the control of the process in place which also covered to the control of the process in place which also covered to the process in place which also covered to the provided to the process in place which also covered to the provided			.,	
3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4 CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational system. Y Y We use mainly infrastructure as code approaches so the software is well tracked. IT inventory all the hardware. Y Y We have CCBs and code change process in place which also cover	1 9 11	N	Y	
clocks with an authoritative source to generate timestamps for audit records. 3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4.1 CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational system. Y Y We use mainly infrastructure as code approaches so the software is well tracked. IT inventory all the hardware. Y Y Y We have CCBs and code change process in place which also cover	, , ,			
3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4 CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational system. Y Y We use mainly infrastructure as code approaches so the software is well tracked. IT inventory all the hardware. Y Y Y We have CCBs and code change process in place which also cover		Y	Y	
modification, and deletion. 3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4 CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. Y Y We use mainly infrastructure as code approaches so the software is well tracked. IT inventory all the hardware. Y Y We have CCBs and code change process in place which also cover			1,,	
3.3.9 Limit management of audit logging functionality to a subset of privileged users. 3.4 CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. Y Y We use mainly infrastructure as code approaches so the software is well tracked. IT inventory all the hardware. Y Y Y We have CCBs and code change process in place which also cover	55 5	Y	Y	
3.4 CONFIGURATION MANAGEMENT 3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. Y Y We have CCBs and code change process in place which also covered to the software is well tracked. IT inventory all the hardware. Y Y Y We have CCBs and code change process in place which also covered to the software is well tracked. IT inventory all the hardware.			1,,	
3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. Y Y We use mainly infrastructure as code approaches so the software is well tracked. IT inventory all the hardware. Y Y We use mainly infrastructure as code approaches so the software is well tracked. IT inventory all the hardware.		Y	Y	
systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems. Well tracked. IT inventory all the hardware. Y Y We have CCBs and code change process in place which also cover				
the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational sys-	ŭ v	Y	Y	11
3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational sys-				well tracked. IT inventory all the hardware.
products employed in organizational systems. 3.4.3 Track, review, approve or disapprove, and log changes to organizational sys-		1		
3.4.3 Track, review, approve or disapprove, and log changes to organizational sys-	, , ,	Y	Y	
		Υ	Y	We have CCBs and code change process in place which also cover
				= ' '



3.4.5 Deficile document, approve, and referre physical sarding gold across reservoines accounted with Anneys to organizational systems. 3.4.7 Respire, the primaple of less functionally by configuring against actional systems to provide only expensional capabilities. 3.4.7 Respire, disable, or prevent the use of increasantial programs, functions, ports, por	3.4.4 Analyze the security impact of changes prior to implementation.	Υ	Υ	
associated with changes to organizational systems. All 6 frency the principle of flees functionality by configuring organizational systems to provide only essential capabilities. All 7 Rentric, disable, or prevent the use of nonescential programs, functions, ports of the provides only essential capabilities. All 7 Rentric, disable, or prevent the use of nonescential programs, functions, ports of the provided				
3.4.5 English, disable, or prevent the use of nonesential programs, functions, ports, protection of productions and positives. 3.4.7 Bestirit, disable, or prevent the use of nonesential programs, functions, ports, protection, and policy developes. 3.4.8 English, developes. 3.4.8 English, developes. 3.4.9 English, developes. 3.4.			'	
to provide only essential capabilities. All Restruct, disable or prevent the use of nonessensial programs, functions, ports, prevance, and services. All Restruct, disable or prevent the use of unauthorized software or drony all, permit by exception (beldisting) policy to prevent the use of unauthorized software or drony all, permit by exception (whelefoling) policy to prevent the use of unauthorized software or drony all, permit by exception (whelefoling) policy to prevent the use of unauthorized software or drony all, permit by exception (whelefoling) policy to prevent the use of unauthorized software. All All Apply captures are software or drony all permit by exception (whelefoling) policy to prevent the use of unauthorized software. All Apply captures are software or drong and the execution of which are all apply and all ap		N	- V	
3.4.7 Recrut, disable, or prevent the use of nonescental programs, fundions, ports, y vector or creative contents. 3.4.8 Apply dely-by-exception (blacklisting) policy to prevent the use of unauthorized between or deally plant by exception (blacklisting) policy to prevent the use of unauthorized software. 3.4.6 Certon and multi-plant by prevent by the use of unauthorized of a section of authorized software. 3.4.6 Certon and multi-plant by exception (blacklisting) policy to allow the excession of authorized software. 3.5.1 Gentral program users, processes acting on behalf of users, and devices. 3.5.1 Authorities or verify the determines of users processes, or devices, as a prevengulate to allowing access to organizational systems. 3.5.1 Use multiplaced authorities on to cold and network access to privileged accounts and for network access to non-privileged accounts. 3.5.6 Employ register authorities of local and network access to privileged accounts. 3.5.6 Provent users of lefetilities for a defined period. N. Y. S. S. Provent users of lefetilities for a defined period. N. Y. Y. S. S. Provent users of lefetilities for a defined period. N. Y. Y. S. S. Provent users of lefetilities for a defined period. N. Y. Y. S. S. Provent users of lefetilities for a defined period. N. Y. Y. S. S. Provent users of lefetilities for a defined period. N. Y. Y. S. S. Provent users of lefetilities for a defined period. N. Y. Y. Y. S. S. Provent users of lefetilities for a defined period. N. Y. Y. Y. S. S. Provent users of a specified number of generators. S. S. Provent users of lefetilities for system indigens with in minimal and complexity and change of characters when new parts of the province of the		IN	Y	
As Apply deproyeespoin (Discussing policy to prevent the use of unauthorized software or denyall, permit-by-exception (whicklisting policy to allow the execution of uniformized software or denyall, permit-by-exception (whicklisting policy to allow the execution of uniformized software). Y Y Y Y Y Y Y Y Y			1,,	
3.4.3 Apply denyby-exception (blacktissing) policy to allow the execution of authorized software. 4.4.4 Coentral and maintior user installed software. 5.1 EVENTIFICATION AND AUTHERTICATION 5.2 Authermicist for verify the identities of users, processes, or devices, as a previous of the international process of processes, or devices, as a previous of the international process of the international process of the international systems. 5.3.1 Identify system users, processes or engineering on behalf of users, and devices, as a previous to a laining access to organized higherts. 5.3.1 Identify system users, processes organized processes, or devices, as a previous to a laining access to organized higherts. 5.3.3 International processes organized access to privileged accounts. 5.3.5 Provent; reads of destrifiers for a defined period. 5.3.5 Provent; read of destrifiers for a defined period of inactivity. 5.3.5 Provent; read of destrifiers for a defined period. 5.3.5 Provent; read of destrifiers for a defined period of inactivity. 5.3.5 Provent; reads of destrifiers for a defined period of inactivity. 5.3.5 Provent; reads of destrifiers for a defined period of inactivity. 5.3.5 Provent; reads of destrifiers for a defined period of inactivity. 5.3.5 Provent; reads of destrifiers for a defined period of inactivity. 5.3.5 Provent; reads of destrifiers for a defined period of inactivity. 7.5 Provent; reads of destrifiers for a defined period of inactivity. 8.3.5 Provent; reads of destrifiers for a specified number of generatories. 7.5 Provent; reads of destrifiers for a defined period of inactivity. 8.3.5 Provent; reads of destrifiers for a defined period of inactivity. 9.7 V.		Y	Y	
software or deny-all, permit-by-exception (whiteking) policy to allow the execution of authorized software. 3.43 Control and monitor user-installed software. 3.45 Control and monitor user-installed software. 3.51 Control software user-processe acting on behalf of users, and devices. 3.51 Control software user-processes acting on behalf of users, and devices. 3.52 Authenticates or verifying the electrical or users, processes, or devices, as a pre-requisite in allowing actives to applicational systems or applicational systems or users are controlled accounts and for network access to organizational systems. 3.54 Employ replay resistant authentication mechanisms for network access to privileged accounts and for network access to apply replay accounts. 3.55 Foverer results of identifiers for a defined period. 3.56 Consideration authentication mechanisms for network access to privileged and mon-privileged accounts. 3.57 Foverer results of identifiers are a defined period. 3.58 Foverer results of identifiers are a defined period. 3.58 Foverer results of identifiers are a defined period of inactives. 3.58 Foverer results of identifiers are a defined period of inactives. 3.58 Foverer results of identifiers are a defined period of inactives. 3.58 Foverer results of identifiers are a defined period of inactives. 3.58 Foverer results are designed accounts. 4.7 Y	1 .			. ,
of authorized software. 4 Y Y 3.5 Intentify speak makes a continuous control processors and of the control processors are created. 5.5 Prowers make of infentiles for an electrol principle and country and of the control processors are created. 5.5 Prowers make of infentiles for an electrol principle and country and of the control processors are created. 5.5 Prowers make of infentiles for an electrol principle and country and of the control processors are created. 5.5 Prowers make of infentiles for an electrol principle and country and processors are created. 5.5 Prowers make of infentiles for an electrol principle and country and processors are a defined point of increase. 7 Y Y 7 Y 7 Y 7 Y 7 Y 8.5 Prowers make of infentiles for an electrol principle and country and processors are a defined point of increase. 8.5 Prowers make of infentiles for a defined principle and country and processors and country and processors are a defined principle and an analysis, contament	3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized	N	Y	We need to implment SUDO lists to restrict access.
3.4.5 Control and monitor user-installed software. 3.5.1 Identify system users processes acting on behalf of users, and devices. 3.5.1 Gentify System users processes acting on behalf of users, and devices. 3.5.2 Authentical or verify the identifies of users, processes, as a pre-requisite to allowing access to organizational systems. 3.5.3 Use multiforan authentication in Food and network access to privileged accounts and for network access to non-privileged accounts. 3.5.6 Employer-payer-scianar authentication for local and network access to privileged and non-privileged accounts. 3.5.6 Provent roses of identifies for a defined period. N. Y. S. S. Provent rose of identifies for a defined period. N. Y. S. S. Provent rose of identifies for a defined period of natury. 3.5.6 Provent rose of identifies for a defined period of natury. 3.5.7 Provent rose of identifies for a defined period. N. Y. Y. S. S. Provent rose of identifies for a defined period. N. Y. Y. S. S. Provent rose of identifies for a defined period of natury. 3.5.8 Provent rose of identifies for provincy and change of characters when new rose of the provincy of	software or deny-all, permit-by-exception (whitelisting) policy to allow the execution			
3.5 Identify sprougers process carring on behalf of users, and devices. 3.5.1 Identify sprougers users, processes acting on behalf of users, and devices. 3.5.3 Use multifactor authentication for local and network access to privileged accounts. 3.5.4 Employ replay-resistant authentication for local and network access to privileged accounts. 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged accounts. 3.5.5 Employ replay-resistant authentication mechanisms for network access to privileged accounts. 3.5.6 Deaths inclinering-ster a defined period. 3.5.7 Employers accounts and for network access to privileged accounts. 3.5.8 Forward results of identifiers for a defined period. 3.5.8 Forward results of identifiers for a defined period. 3.5.8 Forward results of identifiers after a defined period of marcher of the process of	of authorized software.			
3.5.1 Identify system users, processes acting on behalf of users, and devices. 3.5.2 Authentification or verify the identifies of users, processes, or devices, as a pre-regulate to allowing access to organizational systems. 3.5.3 Live multifactor authentication for focal and network access to privileged accounts and for network access to non-privileged accounts. 3.5.6 Employ registers authentification mechanisms for network access to privileged and non-privileged accounts. 3.5.6 Employ registers authentification mechanisms for network access to privileged and non-privileged accounts. 3.5.6 Disable identifiers after a defined period of natctivity. 3.5.6 Disable identifiers after a defined period of natctivity. 3.5.6 Disable identifiers after a defined period of natctivity. 3.5.7 Provent reunal multiple provided accounts. 3.5.8 Provides reunal provided accounts. 3.5.9 Provides reunal provided accounts. 3.5.9 Provides reunal provided accounts. 3.5.10 Sore and reason of case for a specified number of generations. 4.7 Y	3.4.9 Control and monitor user-installed software.	Υ	Υ	
3.5.3 Exemptificate for vertify the literatures of users, processes, or devices, as a pre- requisite to allowing access to organizational systems. 3.5.3 Exemptificator authentication for food and network access to privileged accounts and for network access to mynileged accounts and for network access to mynileged accounts and to metwork access and privileged accounts. 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. 3.5.5 (Disable interings after a defined period. 3.5.5 (Disable interings after a defined period. 3.5.5 (Disable interings after a defined period of matching. 3.5.7 (Disable processor of the period of the period of processor of the period of the period of processor of the period of the	3.5 IDENTIFICATION AND AUTHENTICATION			
3.5.3 Exemptificate for vertify the literatures of users, processes, or devices, as a pre- requisite to allowing access to organizational systems. 3.5.3 Exemptificator authentication for food and network access to privileged accounts and for network access to mynileged accounts and for network access to mynileged accounts and to metwork access and privileged accounts. 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. 3.5.5 (Disable interings after a defined period. 3.5.5 (Disable interings after a defined period. 3.5.5 (Disable interings after a defined period of matching. 3.5.7 (Disable processor of the period of the period of processor of the period of the period of processor of the period of the	3.5.1 Identify system users, processes acting on behalf of users, and devices.	Υ	Y	
requisite to allowing access to organizational systems. 3.5.3 Use multifactor authentication for local and network access to privileged accounts. 3.5.4 Employ registers authentication mechanisms for network access to privileged and non-privileged accounts. 3.5.5 Preview research of intentions of inactivity. 3.5.5 Preview research of inactivity. 3.5.5 Preview research of inactivities of inactivity. 3.5.5 Preview research of inactivities of inactivity. 3.5.5 Provision research of inactivities of inactivity. 3.5.5 Provision ground organization of inactivity. 3.5.5 Provision ground organization information. 3.5.7 Provision ground organization information. 3.6 Inactivities organization organizatio				
3.5.3 Eventurificator authentication for local and network access to provileged accounts and for network access to mynivelized accounts provileged accounts. 3.5.4 Employ replay-sessant authentication mechanisms for network access to provileged accounts. 3.5.5 Prevent reuse of identifiers for a defined period. 3.5.5 Disable demotifiers 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 Provinting password reuse for a specified number of generations. 3.5.9 Allow temporary password reuse for a specified number of generations. 3.5.9 Allow temporary password reuse for a specified number of generations. 3.5.10 Store and transmit only cryptographically-procreed passwords. 3.5.10 Store and ransmit only cryptographically-procreed passwords. 3.5.10 Store and transmit only cryptographically-procreed passwords. 3.5.20 Store and a external to the cognitivation of transmit only cryptographic			'	
courts and for network access to non-privileged accounts. 3.5.4 Employer player-estant authentication mechanisms for network access to privileged and non-privileged accounts. 3.5.6 Prevent research of interfers for a defined period. 3.5.6 Deale 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 Probable identifiers after a defined period of inactivity. 3.5.9 Prevent research of a specified number of generations. 3.5.9 Probable is password reuse for a specified number of generations. 3.5.9 Probable is password reuse for a specified number of generations. 3.5.9 Probable is password reuse for a specified number of generations. 3.5.9 Probable is password reuse for a specified number of generations. 3.5.10 Storce and transmit only coptographically-protected passwords. 3.5.11 Obscure developed the probable of prographically-protected passwords. 3.6.11 Cabable in a operational incident chanding capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activative. 3.6.1 Texability and operational incidents response capability. 3.7.1 Perform maintenance on organizational systems. 3.7.2 Provide cornors on the tools, techniques, mechanisms, and personnel used to conduct system maintenance or organizational systems. 3.7.3 Provide cornors on the tools, techniques, mechanisms, and personnel used to conduct system maintenance or organizational systems. 3.7.3 Provide cornors on the tools, techniques, mechanisms, and personnel used to conduct system maintenance or organizational systems. 3.7.4 Provide cornors on the tools, techniques, mechanisms, and personnel used to conduct system maintenance or organizational systems. 3.7.4 Provide cornors on the tools, techniques, mechanisms, and personnel used to conduct system maintenance or organizational systems. 3.7.5 Provide cornors on the tools, techniques mechanisms on the conductivity of t		N	- V	Lthink chile dent require 25A at the memont
3.5.4 Frovent reuse of identifiers for a defined period. 3.5.5 Prevent reuse of identifiers for a defined period intactive, 3.5.5 Potable destined period intactive, 3.5.7 Force a minimum password complexity and change of characters when new passwords are created. 3.5.8 Flohibit password reuse for a specified number of generations. 3.5.8 Flohibit password reuse for a specified number of generations. 3.5.8 Flohibit password reuse for a specified number of generations. 3.5.9 Flohibit password reuse for a specified number of generations. 3.5.9 Flohibit password rates for a specified number of generations. 3.5.9 Flohibit password rates for a specified number of generations. 3.5.9 Flohibit password rates for a specified number of generations. 3.5.9 Flohibit password rates for a specified number of generations. 3.5.9 Flohibit password rates for a specified number of generations. 3.5.9 Flohibit password rates for a specified number of generations. 3.5.10 Store and transmit only cryptographically protected passwords. 4 Y Y 3.5.10 Store and transmit only cryptographically protected passwords. 5.6.1 Extablish an operational incident handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. 3.6.1 Extablish an operational incident handling capability for organizational systems on the cost in companizational systems. 3.7.1 Perform maintenance on organizational systems. 3.7.2 Flore for maintenance on organizational systems. 3.7.3 Exture adjuncted 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 systems for mailious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance systems or a second part of second password in the password of second password in the password organizational systems. 3.8.1 Protect (Exp. phy		IN	i i	Tullink chile dont require 2FA at the moment
lieged and non-privileged accounts. 3.5. Prevent reuse of identifiers for a defined period. N. Y. 3.5. Provides a constant of the provided of the period of inactivity. 3.5. Provides a constant. 3.5. Provides a contrain of export incidents to designated officials andor authorities both internal and external to the organizational systems. 3.5. Provides controls on the tools, techniques, mechanisms, and personnel used to conduct system maliterature. 3.7. Perform maintenance. 3.7. Perform maintenance are organizational systems. 3.7. Perform maintenance are organizational systems. 3.7. A Perform maintenance are organizational systems. 3.7. Perform maintenance are organizational systems. 3.7. A Perform maintenance are organizational systems. 3.7. A Perform maintenance are organizational systems. 3.7. A Check media are used in organizational systems. 3.7. A Check media are used in organizational systems. 3.7. Sequire multipator outheristication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance are complete. 3.7. Sequire multipator outheristication to establish nonlocal maintenance are complete. 3.7. Sequire multipator outheristication to establish nonlocal maintenance are complete. 3.7. Sequire multipator outheristication to establish nonlocal maintenance are complete. 3.7. Sequire multipator outheristication to establish nonlocal maintenance are complete. 3.7. Sequire multipator outheristication to establish nonlocal maintenance are compl		1	1,,	No. 1 de Com Bill I
3.5.5 Postable identifiers after a defined period of inacticity. 3.5. Floration a minimum password complexity and change of characters when new passwords are created. 3.5. Brothality password results for a specified number of generations. 3.5. Brothality password results for a specified number of generations. 3.5. Postablity password results for a specified number of generations. 3.5. Postablity password use for system logons with an immediate change to a permanent password. 3.5. Postablity password use for system logons with an immediate change to a permanent password. 3.5. Postablity password use for system logons with an immediate change to a permanent password. 3.5. Postablity password use for system logons with an immediate change to a permanent password. 3.5. Postablity password use for system logons with an immediate change to a permanent password. 3.5. Postablity password use for system logons with an immediate change to a permanent password. 3.5. Postablity password use for system logons with an immediate change to a permanent password. 3.5. Postablity password results of the system systems and password. 3.6. Establish and perandian incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. 3.6. Establish and perandian incident-handling capability for organizational systems. 3.6. Tests the organizational incident response capability. 3.7. Almantenan. 3.7. Portion decoration on the tosts, bethriques, mechanisms, and personnel used to conduct system maintenance. 3.7. Portion decoration on the tosts, bethriques, mechanisms, and personnel used to conduct system maintenance. 3.7. Portion maintenance. 3.7. Portion maintenance. 3.7. Portion maintenance. 3.7. Supervise dui organizational systems. 3.7. Supervise dui organizational systems. 3.7. Supervise dui organizational systems. 3.8. Postablity the maintenance activities of maintenance personnel without required access to CUI on system m			Y	Not sure we do this now - Cristian Richard
3.5.0 Fathers a minimum password complexity and change of characters when new passwords are created. 3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created. 3.5.9 Flohibit password reuse for a specified number of generations. 3.5.9 Allow temporary password use for system legons 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. 3.6.1 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 Settle organizational incident response capability. 3.7 MAINTENANCE 3.7.1 Perform maintenance on organizational systems. 26 3.7.2 Provide controls on the tools techniques, mechanisms, and personnel used to conduct system maintenance maintenance and organizational systems. 3.7.3 Require multifactor authorization systems in a maintenance is santitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for maintenance session via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.5 Supervise the maintenance and terminate such connections when nonlocal maintenance is complete. 3.8.6 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI and maintenance personnel with				
3.5.7 Enforce a minimum password complexity and change of characters when new 3.5.8 Prohibit password recreated. 3.5.8 Prohibit password review for a specified number of generations. 3.5.9 Allow rempary password use for a specified number of generations. 3.5.9 Allow rempary password use for system logons with an immediate change to a permanent password. 3.5.10 Store and transmit only cryptographically-protected passwords. 3.5.10 Store and transmit only cryptographically-protected passwords. 3.6.10 Store and transmit on a operational incident-handling capability for organizational systems that includes preparation, detection, nalysis, 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. 3.6.3 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. 3.7.5 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.5 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.5 Provide controls on the tools, techniques mechanisms, and personnel used to conduct system maintenance. 3.7.5 Sequence and in organizational systems. 3.7.5 Sequence and in organizational systems. 3.8 MeDIA PROTECTION 3.8 Protect (e.e., Physically control and securely store) system media containing CUI before disposal or release for received authorities of control and securely store) system media containing CUI before disposal or release for release for release for regular darks of control and securely store) system m	· · · · · · · · · · · · · · · · · · ·			
passwords are created. 3.5 a Prohibit password reuse for a specified number of generations. 7 Y Y Show temporary password use for system logons with an immediate change to a permanent password. 3.5 in Store and transmit only cryptographically protected passwords. 7 Y Y Show the property of a protection of the pro	3.5.6 Disable identifiers after a defined period of inactivity.	Υ	Y	
3.5.9 Allow temporary password use for a specified number of generations. 3.5.10 Shallow 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. 4.7.10 Store and transmit only cryptographically protected passwords. 5.10 Store eleback of authentication information. 7.7.10 Store and transmit only cryptographically protected passwords. 7.7.10 Store and transmit only cryptographically protected passwords. 8.10 Store and transmit only cryptographically protected passwords. 9.7.10 Store and transmit only cryptographical incidents of the cryptographical protection, analysis, containment, recovery, and user response activities. 9.7.2 Store the organizational incident handling capability for organizational systems. 9.7.3 Feat the organizational incident response capability. 9.7.4 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance on organizational systems. 9.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance maintenance in maintenance and containing and passwords. 9.7.2 Provide controls on the tools, techniques, mechanisms for mailcious code before the media arcustification to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 9.7.3 Supervise the maintenance activities of maintenance personnel	3.5.7 Enforce a minimum password complexity and change of characters when new	Y	Υ	
3.5.10 Nov 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 Starbalish an oper attorication information. 3.6.1 NCIDENT RESPONSE 3.6.1 Establish an oper attorial incident-handling capability for organizational systems that includes preparation, descriptor, 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 MANTENANCE 3.7.1 Perform maintenance on organizational systems. 26 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance on organizational reports of the start of the conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is santized 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 multifector authentication to establish nonlocal maintenance is complete. 3.7.5 Separise the maintenance activities of maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.8.1 Entire access to CUI on system media to authorized users. 3.8.2 Fortice (i.e., physically control and securely store) system media containing CUI, both space and digital. 3.8.3 Santize of setury system media containing CUI before disposal or release for reuse. 3.8.4 Mank media with necessary CUI markings and distribution limitations. 27 3.8.5 Control access to media containing cull before disposal or release for reuse. 3.8.6 Prohibit the use of prorable media on system components. 3.8.7 Control the use of removable media on system components. 3.8.9 Protect (i.e., Disposally and provided secretic proposally and media during transport unless otherwise protecte	passwords are created.			
3.5.10 Nov 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 Starbalish an oper attorication information. 3.6.1 NCIDENT RESPONSE 3.6.1 Establish an oper attorial incident-handling capability for organizational systems that includes preparation, descriptor, 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 MANTENANCE 3.7.1 Perform maintenance on organizational systems. 26 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance on organizational reports of the start of the conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is santized 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 multifector authentication to establish nonlocal maintenance is complete. 3.7.5 Separise the maintenance activities of maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.8.1 Entire access to CUI on system media to authorized users. 3.8.2 Fortice (i.e., physically control and securely store) system media containing CUI, both space and digital. 3.8.3 Santize of setury system media containing CUI before disposal or release for reuse. 3.8.4 Mank media with necessary CUI markings and distribution limitations. 27 3.8.5 Control access to media containing cull before disposal or release for reuse. 3.8.6 Prohibit the use of prorable media on system components. 3.8.7 Control the use of removable media on system components. 3.8.9 Protect (i.e., Disposally and provided secretic proposally and media during transport unless otherwise protecte	3.5.8 Prohibit password reuse for a specified number of generations.	Υ	Y	
a permanent password. 3.5.10 Store and transmit only cyptographically protected passwords. Y Y 3.5.10 Control and transmit only cyptographically protected passwords. Y Y Y 3.6 INCIDENT RESPONSE 3.6.10 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 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 Perform maintenance on organizational systems, 26. 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance on organizational systems, 26. 3.7.3 Feature maintenance on off-site maintenance is sanitized of any CUI. 3.7.4 Check media are used in organizational dispositic 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 activities of maintenance activities of maintenance when nonlocal maintenance activities of maintenance activities of maintenance when nonlocal maintenance activities of maintenance ac	<u> </u>			
3.5.11 Discore feedback of authentication information. 3.6 INCIDENT RESPONSE 3.6.1 Estabilish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. 3.6.2 Track, document, and report incidents to designated officials andor authorities both internal and external to the organization. 3.6.3 Test the organizational incident response capability. 3.7 MAINTENANCE 3.7.1 Perform maintenance on organizational systems. 26 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions when 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 (E., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media containing CUI before disposal or release for reuse. 3.8.3 Sanitize or destroy system media containings CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containings CUI and maintenance activities of maintenance is possible and 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 outside of controlled areas. 3.8 Control to use of removable media on system components. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9 Is recent individuals prior to authori			Ι.	
3.5.1 Discure 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 Sets the organizational incident response capability. 3.7.5 Perform maintenance on organizational systems.26 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is santized of any CUI. 3.7.4 Check merit maintenance. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions are 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 and maintenance access to CUI on system media to authorized users. 3.8.2 Limit access to CUI on system media containing CUI before disposal or release for reuse. 3.8.4 MEDIA PROTECTION 3.8.5 Control and media during transport outside of controlled areas. 3.8.5 Control and media during transport outside of controlled areas. 3.8.5 Control and media during transport outside of controlled areas. 3.8.7 Control the use of removable media on system components. 3.8.9 PERSONNEL SECURITY 3.9 PERSONNEL SECURITY 3.9 SPERSONNEL SECURITY 3.9 SPERSONNEL SECURITY	· · · · · · · · · · · · · · · · · · ·	V	- V	
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 Text for organizational incident response capability. 3.7 MAINTENANCE 3.7 MAINTENANCE 3.7.1 Perform maintenance on organizational systems.26 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Fineure 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 was 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 3.8.2 Limit access to CUI on system media containing CUI before disposal or release for reuse. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Nark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to Gui on system media on system components. 3.8.6 Control access to Gui on system media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.7 Control did media during transport authesis there is no removable media on system components. 3.8.9 Frotect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9 S Creen individuals prior to authorizing access to organizational systems contain-				
1.6.1 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. 26 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Frotect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Gontrol 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 outside of controlled areas. 3.8.7 Control the use of removable media on system components. 3.8.9 Fornoit the use of portable storage devices when such devices have no identificable owner. 3.9 PERSONNEL SECURITY 3.9 PERSONNEL SECURITY 3.9 Series individuals prior to authorizing access to organizational systems containin-		Y	Y	
that includes preparation, detection, analysis, containment, recovery, and user response activities. 3.6.2 Track, document, and report incidents to designated officials andor authorities both internal and external to the organization. 3.6.3 Test the organizational incident response capability. 3.7.1 MAINTENAINCE 3.7.1 Perform maintenance on organizational systems.26 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8.1 Entrect (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 destrory system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cytoptographic 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. 3.8.9 Personnet Executive of portable storage devices when such devices have no identificable owner. 3.9 PERSONNEL SECURITY 3.9 PERSONNEL SECURITY 3.9 PERSONNEL SECURITY 3.9 PERSONNEL SECURITY				
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. 3.7.1 Perform maintenance on organizational systems.26 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance on organizational systems.36 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 santized 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 authoritacion 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 Santize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.4 Toolnet the use of removable media on system components. 3.8.7 Control the use of removable media on system components. 3.8.7 Porticle the use of portable storage devices when such devices have no identifiable owner.				
3.6.3 Text characteristics of the organization and external network connections and terminate such connections when nonlocal maintenance activities of maintenance personnel without required access authorization. 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 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 Sanities or destroy system media to authorized users. 3.8.4 Mark media with necessary CUI markings and distribution limitations. 27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.9 PERSONNEL SECURITY 3.9 PERSONNEL SECURITY 3.9 PERSONNEL SECURITY 3.9 1 Screen individuals prior to authorizing access to organizational systems contain-				
both internal and external to the organization. 3.6.3 Test the organizational incident response capability. 3.7 MAINTENANCE 3.7.1 Perform maintenance on organizational systems.26 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 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.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Portect the confidentiality of backup CUI at storage locations. 3.8.9 PERSONNEL SECURITY 3.9 PERSONNEL SECURITY 3.9 1 Screen individuals prior to authorizing access to organizational systems contain-	sponse activities.			
3.6.3 Test the organizational incident response capability. 3.7 MAINTENANCE 3.7.1 Perform maintenance on organizational systems.26 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport uotiside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 PRONNEL SECURITY 3.9 PERSONNEL SECURITY 3.91 Screen individuals prior to authorizing access to organizational systems contain-	3.6.2 Track, document, and report incidents to designated officials andor authorities			
3.7.1 Perform maintenance on organizational systems.26 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.6 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. 3.8.9 PRISONNEL SECURITY 3.9 PERSONNEL SECURITY 3.9 PERSONNEL SECURITY 3.9 15 Green individuals prot to authorizing access to organizational systems contain-	both internal and external to the organization.			
3.7.1 Perform maintenance on organizational systems.26 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.6 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. 3.8.9 PRISONNEL SECURITY 3.9 PERSONNEL SECURITY 3.9 PERSONNEL SECURITY 3.9 15 Green individuals prot to authorizing access to organizational systems contain-	3.6.3 Test the organizational incident response capability.			
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. 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of promovable media on system components. 3.8.9 PROSIONEL SECURITY 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
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. 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of promovable media on system components. 3.8.9 PROSIONEL SECURITY 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
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. 3.8.1 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.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 PROSENISE SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain.				
3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 PROSNDNLS SECURITY 3.9.9 PROSNDNLS SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 PERSONNEL SECURITY 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
the media are used in organizational systems. 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 PROSONEL SECURITY 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 PRESONNEL SECURITY 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-	, ,			
via external network connections and terminate such connections when nonlocal maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 PRESONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 PRESCONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-	via external network connections and terminate such connections when nonlocal			
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.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-	maintenance is complete.			
3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-	3.7.6 Supervise the maintenance activities of maintenance personnel without re-			
3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-	guired access authorization.			
both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-	3.8 MEDIA PROTECTION			
both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-	3.8.1 Protect (i.e., physically control and securely store) system media containing CLII			
3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-	3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI			
3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-	stored on digital media during transport unless otherwise protected by alternative			
3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
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-	, 1			
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-				
3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-			+	
3.9.1 Screen individuals prior to authorizing access to organizational systems contain-				
ing CUI.				
	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.			
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 connec-			
tions with organizational systems and communicating via some other connection to			
resources in external networks (i.e., split tunneling).			
3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of			
CUI during transmission unless otherwise protected by alternative physical safe-			
guards.			
3.13.9 Terminate network connections associated with communications sessions at			
the end of the sessions or after a defined period of inactivity.			
3.13.10 Establish and manage cryptographic keys for cryptography employed in or-			
ganizational systems.			
3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality			
of CUI.			
3.13.12 Prohibit remote activation of collaborative computing devices and provide			
indication of devices in use to users present at the device.29			
3.13.13 Control and monitor the use of mobile code.	Υ	Υ	Currently we have no mobile code
3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technolo-			
gies.			
3.13.15 Protect the authenticity of communications sessions.			
3.13.16 Protect the confidentiality of CUI at rest.	N	Υ	
3.14 SYSTEM AND INFORMATION INTEGRITY			
3.14.1 Identify, report, and correct system flaws in a timely manner.	Υ	Υ	
3.14.2 Provide protection from malicious code at designated locations within organi-	N	N	
zational systems.			
3.14.3 Monitor system security alerts and advisories and take action in response.	Υ	Υ	



3.14.4 Update malicious code protection mechanisms when new releases are avail-	Υ	Υ	
able.			
3.14.5 Perform periodic scans of organizational systems and real-time scans of files	Υ	Υ	
from external sources as files are downloaded, opened, or executed.			
3.14.6 Monitor organizational systems, including inbound and outbound communi-	Υ	Υ	
cations traffic, to detect attacks and indicators of potential attacks.			
Total requirements		108	
Total Rubin Intends to comply with		61	
Total Rubin Complies with in 2021		40	

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

Description
Advanced Encryption Standard
Controlled Unclassified Information
Data Management
DM Technical Note
Department of Energy
Internet Protocol
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