

# Vera C. Rubin Observatory Rubin Observatory Operations

# Pixel Zone system security plan

William O'Mullane

RTN-082

Latest Revision: 2024-07-14

#### DRAFT



# Abstract

This document provides the mapping to NIST800-171 for the Rubin Pixel Zone.





# Change Record

Version	Date	Description	Owner name
0.1	2024-07-05	Initial Draft	William O'Mullane

Document source location: https://github.com/lsst/rtn-082



### Contents

1	Intro	oduction and Scope	1
2	Mini	mum security requirements	1
	2.1	Access Control (AC)	1
	2.2	Awareness and Training (AT)	2
	2.3	Audit and Accountability (AU)	3
	2.4	Certification, Accreditation, and Security Assessments (CA)	3
	2.5	Configuration Management (CM)	3
	2.6	Contingency Planning (CP)	4
	2.7	Identification and Authentication (IA)	4
	2.8	Incident Response (IR)	4
	2.9	Maintenance (MA)	5
	2.10	Media Protection (MP)	5
	2.11	Physical and Environmental Protection (PE)	5
	2.12	Planning (PL)	6
	2.13	Personnel Security (PS)	6
	2.14	Risk Assessment (RA)	6
	2.15	System and Services Acquisition (SA)	7
	2.16	System and Communications Protection (SC)	7
	2.17	System and Information Integrity (SI)	8
A	Com	pliance with NIST800.171	8
В	Refe	rences	19
С	Acro	nyms	20



# Pixel Zone system security plan

## **1** Introduction and Scope

Vera C. Rubin Observatory will observe the night sky with unprecedented frequency and depth. Per DMTN-199, NIST.SP.800-171r3 is applicable to our pixel data. This document provide the security plan for the *Pixel Zone* which encompasses the areas where data is held in NSF facilities. The SLAC facilities are covered in *NEED REF*.

In accordance with NIST.FIPS.200 and DMTN-199 the security category is :

 $SC_{PixelZone} = \{(confidentiality, moderate), (integrity, low), (availability, low)\}$  (1)

The technology implementation details may be found in ITTN-074.

This plan should be reviewed at least annually.

# 2 Minimum security requirements

NIST.FIPS.200 declares 17 security related areas that should be covered, each is given a sub section here. A detailed compliance with NIST.SP.800-171r3 is given in Appendix A. Here we also mention the controls, as outlined in the CUI overlay of NIST.SP.800-171r3, we aim to implement in each section.

#### 2.1 Access Control (AC)

Access to the *Pixel Zone* is restricted to approved account holders. See ITTN-010 and ITTN-045 (AC-01 Policy and Procedures).

Account creation is tracked with Jira tickets and requires manager approval (AC-02 Account Management).

Unix groups are used to restrict individual user access and effectively provide *account types* 

1



(AC-03 Access Enforcement). Sudo is used for escalation by users who are allowed privileged access - use is logged.

DMTN-199 defines the control flow for pixel data (AC-04 Information Flow Enforcement).

Accounts are locked out after 6 failed attempts to log in (AC-07 Unsuccessful Logon Attempts).

Message of the day shall declare the Pixel zone security (Use Notification AC-08).

Sessions are terminated every 24 hours (AC-12 Session Termination).

Remote access is granted via an group membership. 2FA VPN is required for any remote access (remote access AC-17).

Access to summit WiFi is controlled via registered MAC address. Even on the summit WiFi VPN login is required to access the *Pixel Zone* (wireless access AC-18).

We do not allow pixel data to be copied to external devices (External System AC-20).

We have no public access (AC-22 Publicly Accessible Content)

We do not use specific *-admin* accounts - our team is small and we find such accounts less secure.

We shall review group membership for summit access at least once per year.

#### 2.2 Awareness and Training (AT)

The access control plan (Marshall, ACP) indicates training etc. RTN-073 provides guidelines for embargo data access. Specific guidelines on communication channels have been shared with users in DMTN-286. (AT-01 Policy and Procedures)

Embargo training is mandatory for all users with access to pixel data within the embargo period. (AT-02 Literacy Training and Awareness) Training will be renewed annually.



#### 2.3 Audit and Accountability (AU)

An *Observability system* has been built, on contract ITTN-070, to make this information useful to find incursions and anomalies(AU-02 Event Logging, AU-03 Content of Audit Records, AU-07 Audit Record Reduction and Report Generation, AU-12 Audit Record Generation).

Logs shall also be sent to the Research SOC for review (AU-06 Audit Record Review, Analysis, and Reporting).

Audit records have UTC timestamps (AU-08 Time Stamps).

We shall have sufficient log storage, currently 70TB, for 2 years of logs (AU-04 Audit Log Storage Capacity).

Logs shall be kept for at least 2 years (AU-11 Audit Record Retention).

Squadcast is used for alerting on system failures (AU-05 Response to Audit Logging Process Failures).

Logs and audit information are secured for access only by the Chile DevOps team(AU-09 Protection of Audit Information).

#### 2.4 Certification, Accreditation, and Security Assessments (CA)

We are a small team however we regularly assess our security posture and adjust where needed (CA-02 Control Assessments). We shall carry out PEN testing nominally annually but at least every other year. Training was organised for the Chile DevOps team and some individuals will pursue accreditation/certification.

#### 2.5 Configuration Management (CM)

Higher level or broader changes go to an operations CCB RTN-072 (CM-01 Policy and Procedures). Otherwise we run almost exclusively infrastructure as code - our baseline is in github. Changes follow the DM change process - reviews and tests required for any change (CM-03 Configuration Change Control).



The applications deployed and their configurations are all dealt with via our phalanx<sup>1</sup> system (CM-02 Baseline Configuration, CM-08 System Component Inventory).

Pixel data is only located in the pixel zone and embargo rack (CM-12 Information Location).

We do not have a definitions of high-risk areas and therefore we do not apply specific configurations to devices during travel.

#### 2.6 Contingency Planning (CP)

Disaster recovery and incident reporting is covered in RTN-030 (CP-01 Policy and Procedures)

#### 2.7 Identification and Authentication (IA)

IA is covered in ITTN-010 (IA-01 Policy and Procedures). Users are associated with their unique accounts (IA-02 Identification and Authentication). Re-authentication is once per 24 hours (IA-11 Re-Authentication).

Access to the *Pixel Zone* is via 2FA VPN. Devices connection to our networks are know by MAC address.

Typically 1password generated passwords are used and any sharing is done using vaults (IA-05 Authenticator Management). Passwords must by at least 8 chars, use 2 character classes and can not be reused for 10 goes.

All new users are known to admins or confirmed by a manager (IA-12 Identity Proofing).

#### 2.8 Incident Response (IR)

Incident response is covered in RTN-030 §3 (IR-01 Policy and Procedures).

<sup>&</sup>lt;sup>1</sup>https://phalanx.lsst.io



#### 2.9 Maintenance (MA)

We have weekly maintenance windows for summit systems, one each for Infrastructure, Applications, and Control System (MA-01 Policy and Procedures)

Activities are tickets and discussed in stand up meetings (MA-02 Controlled Maintenance).

All tools go through the usual procurement process and maintenance equipment does not and will not hold pixel data (MA-03 Maintenance Tools).

Maintenance is carried out by our personnel (MA-05 Maintenance Personnel).

#### 2.10 Media Protection (MP)

*Pixel Zone* is all about protecting data in the embargo period as per DMTN-199 (MP-01 Policy and Procedures).

Access is controlled via IPA groups and 2Fa VPN (MP-02 Media Access). Data will never be on removable media. We do not allow media to be mounted to machines int he pixel zone.

Pixel data exists on disk in only three locations during the embargo period, there are no further backups of this so no copy on removable media.

#### 2.11 Physical and Environmental Protection (PE)

Computer rooms have key card access and are restricted to a limited number of personnel (PE-02 Physical Access Authorizations, PE-03 Physical Access Control). Racks have further locks and door sensors installed. There are cameras with motion detection functions installed in the computer rooms.

The DWDM (transmission devices) are within the controlled computer room in a locked rack (PE-04 Access Control for Transmission).

Access is logged and logs are kept for up to three years, all the equipment being installed is HID and complies with section 889 of the John S. McCain National Defense Authorization Act



(NDAA) (PE-06 Monitoring Physical Access).

Remote work is allowed from anywhere with access via 2FA VPN (PE-17 Alternate Work Site).

#### 2.12 Planning (PL)

RTN-030 provides pointers to the many information security related documents (PL-01 Policy and Procedures).

Rubin has an acceptable use policy augmented by RTN-073 and DMTN-286 for embargoed data (PL-04 Rules of Behavior).

#### 2.13 Personnel Security (PS)

Only team members will have access to embargo images. All staff are known individuals screened on hiring (PS-01 Policy and Procedures, PS-03 Personnel Screening). In kind contributors working with data are known scientists and all go though FACTs checks to get accounts at USDF.

Where appropriate on termination all account access is removed - some off-boards remain collaborators (PS-04 Personnel Termination).

#### 2.14 Risk Assessment (RA)

This is part of our regular risk assessment process RDO-71 but we also look in depth at specific applications(RA-01 Policy and Procedures).

Mostly we have concentrated the application exposure in phalanx which is carefully assessed and monitored. However we do perform specific security risk assessment where it is considered most needed e.g. SQR-041 for the science platform which is one of our major attack surfaces (RA-03 Risk Assessment).

We have conducted external PEN testing and shall do so annually in addition to using available scanning tools (RA-05 Vulnerability Monitoring and Scanning).



#### 2.15 System and Services Acquisition (SA)

Security for our external facing applications have been encapsulated in Phalanx. (SA-01 Policy and Procedures) This allows a single team to take care of AAA for all applications to minimize the attack surface. The number of applications which can touch the embargoed data is also small and they are behind the 2Fa VPN.

We apply several principles: (SA-08 Security and Privacy Engineering Principles):

- Least Privilege : we try to reduce the number of accounts with privileges
- Minimize attack surface: phalanx really helps with this but also using 2FA and VPN for pixel zone.
- Access control mechanisms: we use tokens for inter application access
- Defense in depth: we are attempting to know when we have been hit
- Open design: our security does not rely on secrecy of design our designs are public
- Economy of mechanism: we always attempt the simplest solution

Our policy is to replace components before they reach EOL (SA-22 Unsupported System Components).

#### 2.16 System and Communications Protection (SC)

DMTN-286 and SITCOMTN-076 cover communication for embargoed data (SC-01 Policy and Procedures).

Embargo data are kept on encrypted disks using OS level encryption (SC-04 Information in Shared System Resources). 2FA VPN is required to access the *Pixel Zone*. We isolate internal traffic on different VLANs. Bastion hosts are used for access to deeper internal systems.

Border firewalls prevent some repeated attacks, confirmed by PEN testing (SC-05 Denial-ofservice Protection, SC-07 Boundary Protection).



Data transmission to SLAC is via secure routers with AES-256 encryption (SC-08 Transmission Confidentiality and Integrity).

Connections are rest each 24 hour period (SC-10 Network Disconnect).

Encryption keys are managed by specific key services (SC-12 Cryptographic Key Establishment and Management).

Embargo data are kept on encrypted disks using OS level encryption at rest (SC-28 Protection of Information at Rest).

#### 2.17 System and Information Integrity (SI)

RTN-030 details specific policies (SI-01 Policy and Procedures).

We respond immediately to any security issue. It receives top priority. Reported vulnerabilities are dealt with within 24 hours (SI-02 Flaw Remediation).

# A Compliance with NIST800.171

Table 1: This table provides an overview of the NIST.SP.800-171r3 and Rubin compliance with it.

NIST 800-171r3	2024 Status	Intended Compli-	Note
		ance	
3.1 ACCESS CONTROL			



	V	L V	
03.01.01 Account Management	Y	Y	IPA groups are in place for summit which restrict privileges of individ-
a. Define the types of system accounts allowed and prohibited.			ual users. Off boarding and account disabling in place - considering
b. Create, enable, modify, disable, and remove system accounts in accordance with			active account with monthly reaffirmation instead. See https://ittn-
policy, procedures, prerequisites, and criteria. c. Specify:			010.lsst.io/
1. Authorized users of the system,			
2. Group and role membership, and			
3. Access authorizations (i.e., privileges) for each account.			
d. Authorize access to the system based on:			
1. A valid access authorization and			
2. Intended system usage.			
e. Monitor the use of system accounts.			
f. Disable system accounts when:			
1. The accounts have expired,			
2. The accounts have been inactive for [Assignment: organization-defined time pe-			
riod],			
3. The accounts are no longer associated with a user or individual,			
<ol><li>The accounts are in violation of organizational policy, or</li></ol>			
5. Significant risks associated with individuals are discovered.			
g. Notify account managers and designated personnel or roles within:			
1. [Assignment: organization-defined time period] when accounts are no longer re-			
quired.			
2. [Assignment: organization-defined time period] when users are terminated or			
transferred.			
3. [Assignment: organization-defined time period] when system usage or the need-			
to-know changes for an individual.			
h. Require that users log out of the system after [Assignment: organization-defined			
time period] of expected inactivity or when [Assignment: organization-defined cir-			
cumstances].			
03.01.02 Access Enforcement Enforce approved authorizations for logical access to	Y	Y	IPA groups are in place on the summit restriiiicting users abilities
CUI and system resources in accordance with applicable access control policies.			Legacy systems use the active directory groups for this.
03.01.03 Information Flow Enforcement Enforce approved authorizations for control-	Y	Y	DMTN-199 defines the control flow for pixel data. Its implentation
ling the flow of CUI within the system and between connected systems.		_	enforces it.
03.01.04 Separation of Duties	Р	P	Principle of least privilege is applied. Some users have access to
a. Identify the duties of individuals requiring separation.			hosts that is unneeded.
b. Define system access authorizations to support separation of duties.		-	
03.01.05 Least Privilege	N	P	Targeted sudo rules are needed for common operations. IPA con-
a. Allow only authorized system access for users (or processes acting on behalf of			trols sudo centrally
users) that is necessary to accomplish assigned organizational tasks.			
b. Authorize access to [Assignment: organization-defined security functions] and [As-			
signment: organization-defined security-relevant information].			
c. Review the privileges assigned to roles or classes of users [Assignment:			
organization-defined frequency] to validate the need for such privileges.			
d. Reassign or remove privileges, as necessary. 03.01.06 Least Privilege – Privileged Accounts	Р	N	These accounts were energifically target in the Comini attack, w
6 6	Р	N	These accounts were specifically target in the Gemini attack - we
a. Restrict privileged accounts on the system to [Assignment: organization-defined			would rather not use this approach.
personnel or roles].			
b. Require that users (or roles) with privileged accounts use non-privileged accounts			
when accessing non-security functions or non-security information.	V	V	
03.01.07 Least Privilege - Privileged Functions	Y	Y	a. sudo must be used for privileged functions
03.01.07 Least Privilege – Privileged Functions a. Prevent non-privileged users from executing privileged functions.	Y	Y	a. sudo must be used for privileged functions b. We log sudo attempts .
03.01.07 Least Privilege – Privileged Functions a. Prevent non-privileged users from executing privileged functions. b. Log the execution of privileged functions.			b. We log sudo attempts .
03.01.07 Least Privilege – Privileged Functions a. Prevent non-privileged users from executing privileged functions. b. Log the execution of privileged functions. 03.01.08 Unsuccessful Logon Attempts	Y	Y Y	b. We log sudo attempts . Web Services such as love, foreman, ipa console, nublado, etc. may
03.01.07 Least Privilege – Privileged Functions a. Prevent non-privileged users from executing privileged functions. b. Log the execution of privileged functions. 03.01.08 Unsuccessful Logon Attempts a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid			<ul> <li>b. We log sudo attempts .</li> <li>Web Services such as love, foreman, ipa console, nublado, etc. main need rate limiting. We don't use passwords in ssh hosts, only ssl</li> </ul>
03.01.07 Least Privilege – Privileged Functions a. Prevent non-privileged users from executing privileged functions. b. Log the execution of privileged functions. 03.01.08 Unsuccessful Logon Attempts a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period].			<ul> <li>b. We log sudo attempts .</li> <li>Web Services such as love, foreman, ipa console, nublado, etc. ma need rate limiting. We don't use passwords in ssh hosts, only ssi keys (which many consider more secure). We are not aware of a retr</li> </ul>
<ul> <li>03.01.07 Least Privilege – Privileged Functions</li> <li>a. Prevent non-privileged users from executing privileged functions.</li> <li>b. Log the execution of privileged functions.</li> <li>03.01.08 Unsuccessful Logon Attempts</li> <li>a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period].</li> <li>b. Automatically [Selection (one or more): lock the account or node for an [Assign-</li> </ul>			<ul> <li>b. We log sudo attempts .</li> <li>Web Services such as love, foreman, ipa console, nublado, etc. ma need rate limiting. We don't use passwords in ssh hosts, only ss keys (which many consider more secure). We are not aware of a retr limit for ssh-key access; an appropriate extra level of security woul</li> </ul>
03.01.07 Least Privilege – Privileged Functions a. Prevent non-privileged users from executing privileged functions. b. Log the execution of privileged functions. 03.01.08 Unsuccessful Logon Attempts a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]. b. Automatically [Selection (one or more): lock the account or node for an [Assign- ment: organization-defined time period]; lock the account or node until released by			<ul> <li>b. We log sudo attempts .</li> <li>Web Services such as love, foreman, ipa console, nublado, etc. main need rate limiting. We don't use passwords in ssh hosts, only ssl keys (which many consider more secure). We are not aware of a retraining for ssh-key access; an appropriate extra level of security would be to not use the default port 22. However, we do limit attempts to the default port 22.</li> </ul>
03.01.07 Least Privilege – Privileged Functions a. Prevent non-privileged users from executing privileged functions. b. Log the execution of privileged functions. 03.01.08 Unsuccessful Logon Attempts a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]]. b. Automatically [Selection (one or more): lock the account or node for an [Assign- ment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other			<ul> <li>b. We log sudo attempts .</li> <li>Web Services such as love, foreman, ipa console, nublado, etc. may need rate limiting. We don't use passwords in ssh hosts, only ssi keys (which many consider more secure). We are not aware of a retry limit for ssh-key access; an appropriate extra level of security would be to not use the default port 22. However, we do limit attempts to 6 with a block of 600 minutes, which will effectively block failed SUDC</li> </ul>
03.01.07 Least Privilege – Privileged Functions a. Prevent non-privileged users from executing privileged functions. b. Log the execution of privileged functions. 03.01.08 Unsuccessful Logon Attempts a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]. b. Automatically [Selection (one or more): lock the account or node for an [Assign- ment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action] when the maximum number of unsuccessful attempts is exceeded.	Y	Y	b. We log sudo attempts . Web Services such as love, foreman, ipa console, nublado, etc. may need rate limiting. We don't use passwords in ssh hosts, only ssh keys (which many consider more secure). We are not aware of a retry limit for ssh-key access; an appropriate extra level of security would be to not use the default port 22. However, we do limit attempts to 6 with a block of 600 minutes, which will effectively block failed SUDC logins.
03.01.07 Least Privilege – Privileged Functions a. Prevent non-privileged users from executing privileged functions. b. Log the execution of privileged functions. 03.01.08 Unsuccessful Logon Attempts a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period], b. Automatically [Selection (one or more): lock the account or node for an [Assign- ment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other			<ul> <li>b. We log sudo attempts .</li> <li>Web Services such as love, foreman, ipa console, nublado, etc. may need rate limiting. We don't use passwords in ssh hosts, only ssh keys (which many consider more secure). We are not aware of a retry limit for ssh-key access; an appropriate extra level of security would be to not use the default port 22. However, we do limit attempts to 6 with a block of 600 minutes, which will effectively block failed SUDC</li> </ul>



03.01.10 Device Lock	Y	Y	This is our policy
	Y	Y	This is our policy.
a. Prevent access to the system by [Selection (one or more): initiating a device lock			
after [Assignment: organization-defined time period] of inactivity; requiring the user			
to initiate a device lock before leaving the system unattended].			
b. Retain the device lock until the user reestablishes access using established identi-			
fication and authentication procedures.			
c. Conceal, via the device lock, information previously visible on the display with a			
publicly viewable image.			
03.01.11 Session Termination.	Y	Y	ssh sessions are generally not limited on hosts but VPN will timeout
Terminate a user session automatically after [Assignment: organization-defined con-			daily; some network equipment has timeouts set;
ditions or trigger events requiring session disconnect].			
03.01.12 Remote Access	Y	Y	We currently check who and from where is connecting. IPA groups
a. Establish usage restrictions, configuration requirements, and connection require-			conrol access (and 2FA VPN). Bastion nodes are used to control
ments for each type of allowable remote system access.			ingress. UNIX groups are used at SLAC for access control.
b. Authorize each type of remote system access prior to establishing such connec-			
tions.			
c. Route remote access to the system through authorized and managed access con-			
trol points.			
d. Authorize the remote execution of privileged commands and remote access to			
security-relevant information.			
03.01.13 Withdrawn	W		Withdrawn in revision 3
03.01.14 Withdrawn	W		Withdrawn in revision 3
03.01.15 Withdrawn	W		Withdrawn in revision 3
03.01.16 Wireless Access	Y	Y	All devices attaching in Chile need to be registered by Mac address.
a. Establish usage restrictions, configuration requirements, and connection require-			We further consider still requiring 2FA VPN to access privileged sys-
ments for each type of wireless access to the system.			tems from the WiFi.
b. Authorize each type of wireless access to the system prior to establishing such			
connections.			
c. Disable, when not intended for use, wireless networking capabilities prior to is-			
suance and deployment.			
d. Protect wireless access to the system using authentication and encryption. 03.01.17 Withdrawn	w		Withdrawn in revision 3
	Y		
03.01.18 Access Control for Mobile Devices	Y	Y	Mobile devices must be registered on the summit - mobile devices
a. Establish usage restrictions, configuration requirements, and connection require-			do not contain pixel data. In the case where an image may exist
ments for mobile devices.			on say commissioning team laptop we will have disk encryption en-
b. Authorize the connection of mobile devices to the system.			abled.
c. Implement full-device or container-based encryption to protect the confidentiality			
of CUI on mobile devices.			
03.01.19 Withdrawn	Y	Y	Withdrawn in revision 3
	Y N	Y Y Y	Withdrawn in revision 3           We use mac address for laptops and personal mobile phones can
03.01.19 Withdrawn			
03.01.19 Withdrawn 03.01.20 Use of External Systems			We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with
03.01.19 Withdrawn 03.01.20 Use of External Systems a. Prohibit the use of external systems unless the systems are specifically authorized.			We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with
03.01.19 Withdrawn 03.01.20 Use of External Systems a. Prohibit the use of external systems unless the systems are specifically authorized. b. Establish the following security requirements to be satisfied on external systems			We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices
03.01.19 Withdrawn 03.01.20 Use of External Systems a. Prohibit the use of external systems unless the systems are specifically authorized. b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assign-			We use mac address for laptops and personal mobile phones car not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices
03.01.19 Withdrawn 03.01.20 Use of External Systems a. Prohibit the use of external systems unless the systems are specifically authorized. b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assign- ment: organization-defined security requirements].			We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices
03.01.19 Withdrawn 03.01.20 Use of External Systems a. Prohibit the use of external systems unless the systems are specifically authorized. b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assign- ment: organization-defined security requirements]. c. Permit authorized individuals to use external systems to access the organizational			We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices
03.01.19 Withdrawn 03.01.20 Use of External Systems a. Prohibit the use of external systems unless the systems are specifically authorized. b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assign- ment: organization-defined security requirements]. c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after: 1. Verifying that the security requirements on the external systems as specified in the			We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices
03.01.19 Withdrawn 03.01.20 Use of External Systems a. Prohibit the use of external systems unless the systems are specifically authorized. b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assign- ment: organization-defined security requirements]. c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after: 1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and			We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices
03.01.19 Withdrawn 03.01.20 Use of External Systems a. Prohibit the use of external systems unless the systems are specifically authorized. b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assign- ment: organization-defined security requirements]. c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after: 1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and 2. Retaining approved system connection or processing agreements with the organi-			We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices
03.01.19 Withdrawn 03.01.20 Use of External Systems a. Prohibit the use of external systems unless the systems are specifically authorized. b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assign- ment: organization-defined security requirements]. c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after: 1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and 2. Retaining approved system connection or processing agreements with the organi- zational entities hosting the external systems.			We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices
03.01.19 Withdrawn 03.01.20 Use of External Systems a. Prohibit the use of external systems unless the systems are specifically authorized. b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assign- ment: organization-defined security requirements]. c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after: 1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and 2. Retaining approved system connection or processing agreements with the organi-			We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices
03.01.19 Withdrawn 03.01.20 Use of External Systems a. Prohibit the use of external systems unless the systems are specifically authorized. b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assign- ment: organization-defined security requirements]. c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after: 1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and 2. Retaining approved system connection or processing agreements with the organi- zational entities hosting the external systems. d. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.	N		We use mac address for laptops and personal mobile phones car not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices on the pixel zone.
03.01.19 Withdrawn 03.01.20 Use of External Systems a. Prohibit the use of external systems unless the systems are specifically authorized. b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assign- ment: organization-defined security requirements]. c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after: 1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and 2. Retaining approved system connection or processing agreements with the organi- zational entities hosting the external systems. d. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems. 03.01.21 Withdrawn	N N V V	Y	We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices on the pixel zone.
03.01.19 Withdrawn         03.01.20 Use of External Systems         a. Prohibit the use of external systems unless the systems are specifically authorized.         b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements].         c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after:         1. Verifying that the security requirements on the external systems as specified in the organization's system connection or processing agreements with the organizational entities hosting the external systems.         d. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.         03.01.21 Withdrawn         03.01.22 Publicly Accessible Content	N		We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices on the pixel zone.           Withdrawn in revision 3           We do not intend to post images on publicly accessible systems.
03.01.19 Withdrawn         03.01.20 Use of External Systems         a. Prohibit the use of external systems unless the systems are specifically authorized.         b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements].         c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after:         1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and         2. Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.         d. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.         03.01.21 Withdrawn         03.01.22 Publicly Accessible Content         a. Train authorized individuals to ensure that publicly accessible information does	N N V V	Y	We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices on the pixel zone.
03.01.19 Withdrawn         03.01.20 Use of External Systems         a. Prohibit the use of external systems unless the systems are specifically authorized.         b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements].         c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after:         1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and         2. Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.         d. Restrict the use of organization-controlled portable storage devices by authorized individuals to ensure that publicly accessible information does not contain CUI.	N N V V	Y	We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices on the pixel zone.         Withdrawn in revision 3         We do not intend to post images on publicly accessible systems.
03.01.19 Withdrawn         03.01.20 Use of External Systems         a. Prohibit the use of external systems unless the systems are specifically authorized.         b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements].         c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after:         1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and         2. Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.         d. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.         03.01.21 Withdrawn         03.01.22 Publicly Accessible Content         a. Train authorized individuals to ensure that publicly accessible information does	N N V V	Y	We use mac address for laptops and personal mobile phones can not connect to the control network. We also have a separation with the LHN SSID and VLANs. We do not allow external storage devices on the pixel zone.         Withdrawn in revision 3         We do not intend to post images on publicly accessible systems.



		1	
03.02.01 Literacy Training and Awareness	Y	Y	A specific course for DMTN-199 is in prep. Each org has cyber secu
a. Provide security literacy training to system users:			rity training already.
1. As part of initial training for new users and [Assignment: organization-defined			
frequency] thereafter,			
2. When required by system changes or following [Assignment: organization-defined			
events], and			
3. On recognizing and reporting indicators of insider threat, social engineering, and			
social mining.			
b. Update security literacy training content [Assignment: organization-defined fre-			
quency] and following [Assignment: organization-defined events].			
03.02.02 Role-Based Training	Р	Y	OUO training at SLAC, DMTN-199 training for commissioners, Spe
a. Provide role-based security training to organizational personnel:			cific training for satellite catalog handlers.
1. Before authorizing access to the system or CUI, before performing assigned duties,			We would like to do more here like capture flag exercises for devel
and [Assignment: organization-defined frequency] thereafter			opers or blue/red teams events.
2. When required by system changes or following [Assignment: organization- defined			Cyber training is annual.
events].			
b. Update role-based training content [Assignment: organization-defined frequency]			
and following [Assignment: organization-defined events].			
03.02.03 Withdrawn	W		Withdrawn in revision 3
3.3 AUDIT AND ACCOUNTABILITY			
03.03.01 Event Logging	Y	Y	Observability contract.
a. Specify the following event types selected for logging within the system: [Assign-			
ment: organization-defined event types].			
b. Review and update the event types selected for logging [Assignment: organization-			
defined frequency].			
	N.	N N	
03.03.02 Audit Record Content a. Include the following content in audit records:	Y	Y	
1. What type of event occurred			
2. When the event occurred			
3. Where the event occurred			
4. Source of the event			
5. Outcome of the event			
6. Identity of the individuals, subjects, objects, or entities associated with the event			
b. Provide additional information for audit records as needed.			
03.03.03 Audit Record Generation	Y	Y	Observability system
a. Generate audit records for the selected event types and audit record content spec-			
ified in 03.03.01 and 03.03.02.			
b. Retain audit records for a time period consistent with the records retention policy.			
03.03.04 Response to Audit Logging Process Failures	N	Y	
a. Alert organizational personnel or roles within [Assignment: organization-defined			
time period] in the event of an audit logging process failure.			
b. Take the following additional actions: [Assignment: organization-defined addi-			
tional actions].			
03.03.05 Audit Record Review, Analysis, and Reporting	N	Y	Again shall look for third party contract for this
a. Review and analyze system audit records [Assignment: organization-defined fre-			
quency] for indications and the potential impact of inappropriate or unusual activity.			
<ul> <li>b. Report findings to organizational personnel or roles.</li> </ul>			
c. Analyze and correlate audit records across different repositories to gain			
organization-wide situational awareness.			
03.03.06 Audit Record Reduction and Report Generation	Y	Y	Observability system
		'	
a. Implement an audit record reduction and report generation capability that sup-			
ports audit record review, analysis, reporting requirements, and after-the-fact inves-			
tigations of incidents.			
b. Preserve the original content and time ordering of audit records.			
03.03.07 Time Stamps	Y	Y	
a. Use internal system clocks to generate time stamps for audit records.			
b. Record time stamps for audit records that meet [Assignment: organization-defined			
granularity of time measurement] and that use Coordinated Universal Time (UTC),			
have a fixed local time offset from UTC, or include the local time offset as part of the			
time stamp.			
03.03.08 Protection of Audit Information	Y	Y	Only specific admin users have access to audit logs
a. Protect audit information and audit logging tools from unauthorized access, mod-			
ification, and deletion.			
b. Authorize access to management of audit logging functionality to only a subset of			
privileged users or roles.			
	147	1	Withdrawn in revision 3
03.03.09 Withdrawn	W		



03.04.01 Baseline Configuration	Y	Y	We use mainly infrastructure as code approaches so the software is
a. Develop and maintain under configuration control, a current baseline configura-			well tracked. IT inventory all the hardware.
tion of the system.			
b. Review and update the baseline configuration of the system [Assignment:			
organization-defined frequency] and when system components are installed or mod-			
ified.			
03.04.02 Configuration Settings	Y	Y	ConConfiguration settings are defined and documented in the lsst-it
a. Establish, document, and implement the following configuration settings for the			rancher, puppet and phalanx repos.
system that reflect the most restrictive mode consistent with operational require-			rancher, pupper and phalanx repos.
ments: [Assignment: organization-defined configuration settings].			
b. Identify, document, and approve any deviations from established configuration			
settings.			
03.04.03 Configuration Change Control	Y	Y	We have an operatons CCB (https://rtn-072.lsst.io/) and code change
a. Define the types of changes to the system that are configuration-controlled.			process in place which also cover the infrastructure as code.
b. Review proposed configuration-controlled changes to the system, and approve or			
disapprove such changes with explicit consideration for security impacts.			
c. Implement and document approved configuration-controlled changes to the sys-			
tem.			
d. Monitor and review activities associated with configuration-controlled changes to			
the system.			
03.04.04 Impact Analyses	Y	Y	Continuous integrations checks on number and phalany shack any
	Ť	ř	Continuous integrations checks on puppet and phalanx check any
a. Analyze changes to the system to determine potential security impacts prior to			changes prior to test deploy which is done prior to production.
change implementation.			
b. Verify that the security requirements for the system continue to be satisfied after			
the system changes have been implemented.			
03.04.05 Access Restrictions for Change	Y	Y	At infrastructure level this is is controlled by the Chile DevOps team.
Define, document, approve, and enforce physical and logical access restrictions asso-			
ciated with changes to the system.			
03.04.06 Least Functionality	Y	Y	Most application level functionality is controlled via phalanx. The OS
a. Configure the system to provide only mission-essential capabilities.			level is puppet controlled.
b. Prohibit or restrict use of the following functions, ports, protocols, connections, and			
services: [Assignment: organization-defined functions, ports, protocols, connections,			
and services].			
c. Review the system [Assignment: organization-defined frequency] to identify un-			
necessary or nonsecure functions, ports, protocols, connections, and services.			
d. Disable or remove functions, ports, protocols, connections, and services that are			
unnecessary or nonsecure.			
03.04.07 Withdrawn	W		Withdrawn in revision 3
03.04.08 Authorized Software – Allow by Exception	Y	Y	SUDO lists restrict access so users can not install applications on the
a. Identify software programs authorized to execute on the system.			summit nor in SLAC (outside a container). Mainly we containerize
b. Implement a deny-all, allow-by-exception policy for the execution of authorized			the applications and have users work within deployed containers.
software programs on the system.			
			All containers are controlled/deployed via phalanx configuration.
c. Review and update the list of authorized software programs [Assignment:			
organization-defined frequency].			
03.04.09 Withdrawn	W		Withdrawn in revision 3
03.04.10 System Component Inventory	Y	Y	phalanx.lsst.io
a. Develop and document an inventory of system components.			
b. Review and update the system component inventory [Assignment: organization-			
defined frequency].			
c. Update the system component inventory as part of installations, removals, and			
system updates.			
	Y	+ v	DMTN 100 Embargo rack and nivel zones are our places for re-
03.04.11 Information Location	T	Y	DMTN-199- Embargo rack and pixel zones are our places for re-
a. Identify and document the location of CUI and the system components on which			stricted items.
the information is processed and stored.			
b. Document changes to the system or system component location where CUI is pro-			
cessed and stored.			
03.04.12 System and Component Configuration for High-Risk Areas	N	N	Though people self select to remove vaults and carry clean personal
a. Issue systems or system components with the following configurations to individ-			devices we do not have a strict policy nor do we have a list of high
			risk areas. In general there is no data on peoples machines so it is
uals traveling to high-risk locations: [Assignment: organization-defined system con-			
uals traveling to high-risk locations: [Assignment: organization-defined system con-			
figurations].			account/password vulnerability we would need to cover.
figurations]. b. Apply the following security requirements to the systems or components when the			
figurations]. b. Apply the following security requirements to the systems or components when the individuals return from travel: [Assignment: organization-defined security require-			
figurations]. b. Apply the following security requirements to the systems or components when the			



03.05.01 User Identification and Authentication	Y	Y	Users are associated with their unique Unix accounts.
a. Uniquely identify and authenticate system users, and associate that unique identi-			Re-authentication is once per 24 hours.
fication with processes acting on behalf of those users.			
b. Re-authenticate users when [Assignment: organization-defined circumstances or			
situations requiring re-authentication].			
03.05.02 Device Identification and Authentication	Y	Y	Users access via VPN with a 2FA device (DUO or 1password)
		'	Users access via very with a 2PA device (DOO of Tpassword)
Uniquely identify and authenticate [Assignment: organization-defined devices or			
types of devices] before establishing a system connection.			
03.05.03 Multi-Factor Authentication	Y	Y	Summit uses 2FA - SLAC do no require this.
Implement multi-factor authentication for access to privileged and non-privileged ac-			
counts.			
03.05.04 Replay-Resistant Authentication	Y	Y	Lockout after six failures.
Implement replay-resistant authentication mechanisms for access to privileged and			
non-privileged accounts.			
03.05.05 Identifier Management	Y	Y	a. Jira tickets are used and management approval requested
a. Receive authorization from organizational personnel or roles to assign an individ-			b. Unique id is chosen
ual, group, role, service, or device identifier.			c. last 10 passwords can not be used
b. Select and assign an identifier that identifies an individual, group, role, service, or			d. Single sign on across all systems uses same id.
device.			See also https://ittn-045.lsst.io/
c. Prevent the reuse of identifiers for [Assignment: organization-defined time period].			
d. Manage individual identifiers by uniquely identifying each individual as [Assign-			
ment: organization-defined characteristic identifying individual status].			
03.05.06 Withdrawn	W		Withdrawn in revision 3
03.05.07 Password Management	Y	Y	a. For the few system passwords we have a gnerator is used such as
a. Maintain a list of commonly-used, expected, or compromised passwords, and up-			1password.
date the list [Assignment: organization-defined frequency] and when organizational			b. We do use https://haveibeenpwned.com/Passwords
passwords are suspected to have been compromised.			c. Passwords than must be shared are shared via 1password vaults.
b. Verify that passwords are not found on the list of commonly used, expected, or			For users onetimesecret is used to pass an initial password which
compromised passwords when users create or update passwords.	/		must then be replaced.
c. Transmit passwords only over cryptographically protected channels.			d. 1password is used for passwords
d. Store passwords in a cryptographically protected form.			e. account recovery typically starts with a new password the user
e. Select a new password upon first use after account recovery.			must then replace.
f. Enforce the following composition and complexity rules for passwords: [Assign-			f. complex passwords are required.
ment: organization-defined composition and complexity rules].			
03.05.08 Withdrawn	W		Withdrawn in revision 3
03.05.09 Withdrawn	W		Withdrawn in revision 3
03.05.10 Withdrawn	W		Withdrawn in revision 3
03.05.11 Authentication Feedback	Y	Y	Passwords are not echoed on any system.
		1	rasswords are not echoed on any system.
Obscure feedback of authentication information during the authentication process.			
03.05.12 Authenticator Management	Y	Y	This applies mainly to passwords for us. We pass passwords with
a. Verify the identity of the individual, group, role, service, or device receiving the			onetimesecret and then ask the user to change it immediately.
authenticator as part of the initial authenticator distribution.			
b. Establish initial authenticator content for any authenticators issued by the organi-			
zation.			
zation. c. Establish and implement administrative procedures for initial authenticator distri-			
zation.			
zation. c. Establish and implement administrative procedures for initial authenticator distri-			
zation. c. Establish and implement administrative procedures for initial authenticator distri- bution; for lost, compromised, or damaged authenticators; and for revoking authen-			
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> </ul>			
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency]</li> </ul>			
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> </ul>			
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> </ul>			
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> </ul>			
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> </ul>	Y	Y	Inceident hadling/response is in place.
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> </ul>	Y	Y	Inceident hadling/response is in place. AURA also have insurance for serious incursions.
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> <li>03.06.01 Incident Handling</li> </ul>	Y	Y	
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> <li>03.06.01 Incident Handling</li> <li>Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradi-</li> </ul>	Y	Y	
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> <li>03.06.01 Incident Handling</li> <li>Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.</li> </ul>			AURA also have insurance for serious incursions.
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> <li>03.06.01 Incident Handling</li> <li>Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.</li> <li>03.06.02 Incident Monitoring, Reporting, and Response Assistance</li> </ul>	 Y Y	Y Y Y	AURA also have insurance for serious incursions. We track and report incidents.
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> <li>03.06.01 Incident Handling</li> <li>Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.</li> <li>03.06.02 Incident Monitoring, Reporting, and Response Assistance <ul> <li>a. Track and document system security incidents.</li> </ul> </li> </ul>			AURA also have insurance for serious incursions.
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> <li>03.06.01 Incident Handling</li> <li>Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.</li> <li>03.06.02 Incident Monitoring, Reporting, and Response Assistance</li> <li>a. Track and document system security incidents.</li> <li>b. Report suspected incidents to the organizational incident response capability</li> </ul>			AURA also have insurance for serious incursions. We track and report incidents.
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> <li>03.06.01 Incident Handling</li> <li>Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.</li> <li>03.06.02 Incident Monitoring, Reporting, and Response Assistance <ul> <li>a. Track and document system security incidents.</li> </ul> </li> </ul>			AURA also have insurance for serious incursions. We track and report incidents.
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> <li>03.06.01 Incident Handling</li> <li>Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.</li> <li>03.06.02 Incident Monitoring, Reporting, and Response Assistance</li> <li>a. Track and document system security incidents.</li> <li>b. Report suspected incidents to the organizational incident response capability</li> </ul>			AURA also have insurance for serious incursions. We track and report incidents.
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> <li>03.06.01 Incident Handling</li> <li>Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.</li> <li>03.06.02 Incident Monitoring, Reporting, and Response Assistance</li> <li>a. Track and document system security incidents.</li> <li>b. Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period].</li> <li>c. Report incident information to [Assignment: organization-defined authorities].</li> </ul>			AURA also have insurance for serious incursions. We track and report incidents.
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> <li>03.06.01 Incident Handling</li> <li>Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.</li> <li>03.06.02 Incident Monitoring, Reporting, and Response Assistance</li> <li>a. Track and document system security incidents.</li> <li>b. Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period].</li> <li>c. Report incident information to [Assignment: organization-defined authorities].</li> <li>d. Provide an incident response support resource that offers advice and assistance</li> </ul>			AURA also have insurance for serious incursions. We track and report incidents.
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> <li>03.06.01 Incident Handling</li> <li>Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.</li> <li>03.06.02 Incident Monitoring, Reporting, and Response Assistance <ul> <li>a. Track and document system security incidents.</li> <li>b. Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined authorities].</li> <li>d. Provide an incident response support resource that offers advice and assistance to system users on handling and reporting incidents.</li> </ul> </li> </ul>	Y	Y	AURA also have insurance for serious incursions. We track and report incidents. AURA insurance can provide furhter support if needed.
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> <li>03.06.01 Incident Handling</li> <li>Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.</li> <li>03.06.02 Incident Monitoring, Reporting, and Response Assistance <ul> <li>a. Track and document system security incidents.</li> <li>b. Report suspected incidents to the organization-defined authorities].</li> <li>d. Provide an incident response support resource that offers advice and assistance to system users on handling and reporting incidents.</li> </ul> </li> </ul>			AURA also have insurance for serious incursions. We track and report incidents.
<ul> <li>zation.</li> <li>c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.</li> <li>d. Change default authenticators at first use.</li> <li>e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].</li> <li>f. Protect authenticator content from unauthorized disclosure and modification.</li> <li>3.6 INCIDENT RESPONSE</li> <li>03.06.01 Incident Handling</li> <li>Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.</li> <li>03.06.02 Incident Monitoring, Reporting, and Response Assistance</li> <li>a. Track and document system security incidents.</li> <li>b. Report suspected incidents to the organization-defined authorities].</li> <li>d. Provide an incident response support resource that offers advice and assistance to system users on handling and reporting incidents.</li> </ul>	Y	Y	AURA also have insurance for serious incursions. We track and report incidents. AURA insurance can provide furhter support if needed.



03.06.04 Incident Response Training	Y	Y	Cyber training includes user level incedent response i.e. who to re
a. Provide incident response training to system users consistent with assigned roles	l		port attempts to.
and responsibilities:			
1. Within [Assignment: organization-defined time period] of assuming an incident			
	1		
response role or responsibility or acquiring system access,			
<ol><li>When required by system changes, and</li></ol>	1		
<ol><li>[Assignment: organization-defined frequency] thereafter.</li></ol>	1		
b. Review and update incident response training content [Assignment: organization-			
defined frequency] and following [Assignment: organization-defined events].	1		
03.06.05 Incident Response Plan	Y	Y	RTN-030 Section 3.
·		I T	KTN-050 Section 5.
a. Develop an incident response plan that:	1		
1. Provides the organization with a roadmap for implementing its incident response	1		
capability,	1		
<ol><li>Describes the structure and organization of the incident response capability,</li></ol>			
3. Provides a high-level approach for how the incident response capability fits into	1		
the overall organization,			
	1		
4. Defines reportable incidents,	1		
<ol><li>Addresses the sharing of incident information, and</li></ol>	1		
<ol><li>Designates responsibilities to organizational entities, personnel, or roles.</li></ol>	1		
b. Distribute copies of the incident response plan to designated incident response	1		
personnel (identified by name and/or by role) and organizational elements.	1		
c. Update the incident response plan to address system and organizational changes	1		
or problems encountered during plan implementation, execution, or testing.	1		
<ol> <li>Protect the incident response plan from unauthorized disclosure.</li> </ol>	L		
3.7 MAINTENANCE			
03.07.01 Withdrawn	W		Withdrawn in revision 3
03.07.02 Withdrawn	W		Withdrawn in revision 3
	W		
03.07.03 Withdrawn		4	Withdrawn in revision 3
03.07.04 Maintenance Tools	Y	Y	a. Maintenance tools go through the requisition process - hence a
a. Approve, control, and monitor the use of system maintenance tools.	1		least 2 managers approve.
b. Check media with diagnostic and test programs for malicious code before it is used	1		b. We run scans on downloaded media.
in the system.	1		c. Maintenance equipment does not have CUI on it.
c. Prevent the removal of system maintenance equipment containing CUI by verifying			
that there is no CUI on the equipment, sanitizing or destroying the equipment, or			
retaining the equipment within the facility.			
03.07.05 Nonlocal Maintenance	Y	Y	a. Activities are always Jira ticketed
a. Approve and monitor nonlocal maintenance and diagnostic activities.	1		b. 2FA is always needed to access pixel zone.
b. Implement multi-factor authentication and replay resistance in the establishment	1		c. Policy is to log off when done.
			c. Folicy is to log on when done.
of nonlocal maintenance and diagnostic sessions.	1		
c. Terminate session and network connections when nonlocal maintenance is com-			
pleted.			
03.07.06 Maintenance Personnel	Y	Y	In general our staff do the maintenance. On occasion when we hav
03.07.06 Maintenance Personnel	Y	Y	
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization.	Y	Y	remote assistance credentials are granted for a limited time an
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel.	Y	Y	
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos-	Y	Y	remote assistance credentials are granted for a limited time an
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations.	Y	Y	remote assistance credentials are granted for a limited time an
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos-	Y	Y	remote assistance credentials are granted for a limited time an
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION	Y	Y	remote assistance credentials are granted for a limited time an work is carried out with our staff.
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage			remote assistance credentials are granted for a limited time an
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI.	Y	Y	remote assistance credentials are granted for a limited time an work is carried out with our staff. Pixel Zone and Embago Rack
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access			remote assistance credentials are granted for a limited time an work is carried out with our staff.
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles.	Y	Y	remote assistance credentials are granted for a limited time an work is carried out with our staff. Pixel Zone and Embago Rack
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access	Y	Y	remote assistance credentials are granted for a limited time an work is carried out with our staff. Pixel Zone and Embago Rack
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles. 03.08.03 Media Sanitization	Y	Y Y Y	remote assistance credentials are granted for a limited time an work is carried out with our staff. Pixel Zone and Embago Rack Pixel Zone and Embago Rack
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles. 03.08.03 Media Sanitization Sanitize system media that contain CUI prior to disposal, release out of organizational	Y	Y Y Y	remote assistance credentials are granted for a limited time an work is carried out with our staff. Pixel Zone and Embago Rack Pixel Zone and Embago Rack
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles. 03.08.03 Media Sanitization Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse.	Y Y Y	Y Y Y Y	remote assistance credentials are granted for a limited time an work is carried out with our staff. Pixel Zone and Embago Rack Pixel Zone and Embago Rack We format/clean all devices prior to disposal/reuse.
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles. 03.08.03 Media Sanitization Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse. 03.08.04 Media Marking	Y	Y Y Y	remote assistance credentials are granted for a limited time an work is carried out with our staff. Pixel Zone and Embago Rack Pixel Zone and Embago Rack
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles. 03.08.03 Media Sanitization Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse.	Y Y Y	Y Y Y Y	remote assistance credentials are granted for a limited time ar work is carried out with our staff. Pixel Zone and Embago Rack Pixel Zone and Embago Rack We format/clean all devices prior to disposal/reuse.
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles. 03.08.03 Media Sanitization Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse. 03.08.04 Media Marking	Y Y Y	Y Y Y Y	remote assistance credentials are granted for a limited time ar work is carried out with our staff. Pixel Zone and Embago Rack Pixel Zone and Embago Rack We format/clean all devices prior to disposal/reuse.
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles. 03.08.03 Media Sanitization Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse. 03.08.04 Media Marking Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings.	Y Y Y Y	Y Y Y Y Y	remote assistance credentials are granted for a limited time ar work is carried out with our staff. Pixel Zone and Embago Rack Pixel Zone and Embago Rack We format/clean all devices prior to disposal/reuse. We do not use any removable media for embargo information.
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles. 03.08.03 Media Sanitization Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse. 03.08.04 Media Marking Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings. 03.08.05 Media Transport	Y Y Y	Y Y Y Y	remote assistance credentials are granted for a limited time ar work is carried out with our staff. Pixel Zone and Embago Rack Pixel Zone and Embago Rack We format/clean all devices prior to disposal/reuse. We do not use any removable media for embargo information. We do not use any removable media for embargo information.
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles. 03.08.03 Media Sanitization Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse. 03.08.04 Media Marking Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings. 03.08.05 Media Transport a. Protect and control system media that contain CUI during transport outside of	Y Y Y Y	Y Y Y Y Y	remote assistance credentials are granted for a limited time ar work is carried out with our staff. Pixel Zone and Embago Rack Pixel Zone and Embago Rack We format/clean all devices prior to disposal/reuse. We do not use any removable media for embargo information.
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles. 03.08.03 Media Sanitization Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse. 03.08.04 Media Marking Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings. 03.08.05 Media Transport a. Protect and control system media that contain CUI during transport outside of controlled areas.	Y Y Y Y	Y Y Y Y Y	remote assistance credentials are granted for a limited time ar work is carried out with our staff. Pixel Zone and Embago Rack Pixel Zone and Embago Rack We format/clean all devices prior to disposal/reuse. We do not use any removable media for embargo information. We do not use any removable media for embargo information.
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles. 03.08.03 Media Sanitization Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse. 03.08.04 Media Marking Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings. 03.08.05 Media Transport a. Protect and control system media that contain CUI during transport outside of	Y Y Y Y	Y Y Y Y Y	remote assistance credentials are granted for a limited time ar work is carried out with our staff. Pixel Zone and Embago Rack Pixel Zone and Embago Rack We format/clean all devices prior to disposal/reuse. We do not use any removable media for embargo information. We do not use any removable media for embargo information.
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles. 03.08.03 Media Sanitization Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse. 03.08.04 Media Marking Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings. 03.08.05 Media Transport a. Protect and control system media that contain CUI during transport outside of controlled areas.	Y Y Y Y	Y Y Y Y Y	remote assistance credentials are granted for a limited time an work is carried out with our staff.  Pixel Zone and Embago Rack  Pixel Zone and Embago Rack  We format/clean all devices prior to disposal/reuse.  We do not use any removable media for embargo information.  We do not use any removable media for embargo information.
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles. 03.08.03 Media Sanitization Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse. 03.08.04 Media Marking Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings. 03.08.05 Media Transport a. Protect and control system media that contain CUI during transport outside of controlled areas. b. Maintain accountability of system media that contain CUI during transport outside of controlled areas.	Y Y Y Y	Y Y Y Y Y	remote assistance credentials are granted for a limited time an work is carried out with our staff.  Pixel Zone and Embago Rack  Pixel Zone and Embago Rack  We format/clean all devices prior to disposal/reuse.  We do not use any removable media for embargo information.  We do not use any removable media for embargo information. A
03.07.06 Maintenance Personnel a. Establish a process for maintenance personnel authorization. b. Maintain a list of authorized maintenance organizations or personnel. c. Verify that non-escorted personnel who perform maintenance on the system pos- sess the required access authorizations. 3.8 MEDIA PROTECTION 03.08.01 Media Storage Physically control and securely store system media that contain CUI. 03.08.02 Media Access Restrict access to CUI on system media to authorized personnel or roles. 03.08.03 Media Sanitization Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse. 03.08.04 Media Marking Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings. 03.08.05 Media Transport a. Protect and control system media that contain CUI during transport outside of controlled areas. b. Maintain accountability of system media that contain CUI during transport outside	Y Y Y Y	Y Y Y Y Y	remote assistance credentials are granted for a limited time ar work is carried out with our staff. Pixel Zone and Embago Rack Pixel Zone and Embago Rack We format/clean all devices prior to disposal/reuse. We do not use any removable media for embargo information. We do not use any removable media for embargo information.



03.08.07 Media Use	N	Y	Can be rolled out with puppet but there are some servers require
a. Restrict or prohibit the use of [Assignment: organization-defined types of system			USB to be enabled but are in the server room. We can disable USB
media].			disk mounts at OS level. The machines and filesystem are encrypted
b. Prohibit the use of removable system media without an identifiable owner.			so even if someone rebooted a node from a device to allow mount-
			ing USB they still could not get any data.
03.08.08 Withdrawn	W		Withdrawn in revision 3
03.08.09 System Backup – Cryptographic Protection	Y	Y	Pixel data is in only three locations - two in Chile and SLAC. There are
a. Protect the confidentiality of backup information.			no backups during embargo.
b. Implement cryptographic mechanisms to prevent the unauthorized disclosure of			
CUI at backup storage locations.			
3.9 PERSONNEL SECURITY			
03.09.01 Personnel Screening	Y	Y	Only project team members will have access to early images - all are
a. Screen individuals prior to authorizing access to the system.			known individuals screened on hiring. This doesn't suggest b
b. Rescreen individuals in accordance with [Assignment: organization-defined condi-			ground security screening and it was also explicitly not required by
tions requiring rescreening].			the agencies in section 2 of the requirements document.
03.09.02 Personnel Termination and Transfer	Y	Y	This is the offbording policy. Note that many collaborators retain
a. When individual employment is terminated:			some level of access even when offbarded.
			some level of access even when of barded.
1. Disable system access within [Assignment: organization-defined time period],			
2. Terminate or revoke authenticators and credentials associated with the individual,			
and			
3. Retrieve security-related system property.			
b. When individuals are reassigned or transferred to other positions in the organiza-			
tion:			
1. Review and confirm the ongoing operational need for current logical and physical			
access authorizations to the system and facility, and			
2. Modify access authorization to correspond with any changes in operational need.			
3.10 PHYSICAL PROTECTION			
03.10.01 Physical Access Authorizations	Y	Y	This physical access includes locks on server cabinets and key card
a. Develop, approve, and maintain a list of individuals with authorized access to the			access in base. (Contracted for summit computer room)
facility where the system resides.			
b. Issue authorization credentials for facility access.			
c. Review the facility access list [Assignment: organization-defined frequency].			
d. Remove individuals from the facility access list when access is no longer required.			
03.10.02 Monitoring Physical Access	Y	Y	Security is in place on Cero Pachon and at the entrance to the moun-
a. Monitor physical access to the facility where the system resides to detect and re-			tain - though not only for Rubin so not permanently at the observa-
spond to physical security incidents.			tory.
b. Review physical access logs [Assignment: organization-defined frequency] and			tory.
upon occurrence of [Assignment: organization-defined events or potential indica-			
tions of events].	14/		Mithelencer in production 2
03.10.03 Withdrawn	W		Withdrawn in revision 3
03.10.04 Withdrawn	W		Withdrawn in revision 3
03.10.05 Withdrawn	W		Withdrawn in revision 3
03.10.06 Alternate Work Site	Y	Y	All work can be done remotely from any location via the 2FA VPN.
<ul> <li>Determine alternate work sites allowed for use by employees.</li> </ul>			Cyber training assumes remote work is common.
b. Employ the following security requirements at alternate work sites: [Assignment:			
organization-defined security requirements].			
03.10.07 Physical Access Control	Y	Y	a. Computer centers are restricted with key cards to appropriate
a. Enforce physical access authorizations at entry and exit points to the facility where			staff - contractors are considered like staff.
the system resides by:			b. NOIRLab can currently store 80 gigs of data for audit logs of phys-
1. Verifying individual physical access authorizations before granting access to the			ical access, which will last at least three years - all the equipment
facility and			being installed is HID and complies with section 889 of the John S.
facility and 2. Controlling ingress and egress with physical access control systems, devices, or			being installed is HID and complies with section 889 of the John S. McCain National Defense Authorization Act (NDAA)
2. Controlling ingress and egress with physical access control systems, devices, or			McCain National Defense Authorization Act (NDAA)
2. Controlling ingress and egress with physical access control systems, devices, or guards.			McCain National Defense Authorization Act (NDAA) c. visitors are escorted where appropriate i.e. where we have secure
<ul><li>2. Controlling ingress and egress with physical access control systems, devices, or guards.</li><li>b. Maintain physical access audit logs for entry or exit points.</li></ul>			McCain National Defense Authorization Act (NDAA) c. visitors are escorted where appropriate i.e. where we have secure hardware.
<ul><li>2. Controlling ingress and egress with physical access control systems, devices, or guards.</li><li>b. Maintain physical access audit logs for entry or exit points.</li><li>c. Escort visitors, and control visitor activity.</li></ul>			McCain National Defense Authorization Act (NDAA) c. visitors are escorted where appropriate i.e. where we have secure hardware. d. Individuals have cards/keys they are not left in insecure locations.
<ul> <li>2. Controlling ingress and egress with physical access control systems, devices, or guards.</li> <li>b. Maintain physical access audit logs for entry or exit points.</li> <li>c. Escort visitors, and control visitor activity.</li> <li>d. Secure keys, combinations, and other physical access devices.</li> </ul>			McCain National Defense Authorization Act (NDAA) c. visitors are escorted where appropriate i.e. where we have secure hardware.
<ol> <li>Controlling ingress and egress with physical access control systems, devices, or guards.</li> <li>Maintain physical access audit logs for entry or exit points.</li> <li>Escort visitors, and control visitor activity.</li> <li>Secure keys, combinations, and other physical access devices.</li> <li>Control physical access to output devices to prevent unauthorized individuals from</li> </ol>			McCain National Defense Authorization Act (NDAA) c. visitors are escorted where appropriate i.e. where we have secure hardware. d. Individuals have cards/keys they are not left in insecure locations.
<ol> <li>Controlling ingress and egress with physical access control systems, devices, or guards.</li> <li>Maintain physical access audit logs for entry or exit points.</li> <li>Escort visitors, and control visitor activity.</li> <li>Secure keys, combinations, and other physical access devices.</li> <li>Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.</li> </ol>			McCain National Defense Authorization Act (NDAA) c. visitors are escorted where appropriate i.e. where we have secure hardware. d. Individuals have cards/keys they are not left in insecure locations. e. we will not be printing images.
<ol> <li>Controlling ingress and egress with physical access control systems, devices, or guards.</li> <li>Maintain physical access audit logs for entry or exit points.</li> <li>Escort visitors, and control visitor activity.</li> <li>Secure keys, combinations, and other physical access devices.</li> <li>Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.</li> <li>03.10.08 Access Control for Transmission</li> </ol>	Y	Y	McCain National Defense Authorization Act (NDAA) c. visitors are escorted where appropriate i.e. where we have secure hardware. d. Individuals have cards/keys they are not left in insecure locations e. we will not be printing images. DWDM, secure routers are in card controlled room (summit contract
<ul> <li>2. Controlling ingress and egress with physical access control systems, devices, or guards.</li> <li>b. Maintain physical access audit logs for entry or exit points.</li> <li>c. Escort visitors, and control visitor activity.</li> <li>d. Secure keys, combinations, and other physical access devices.</li> <li>e. Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.</li> <li>03.10.08 Access Control for Transmission</li> <li>Control physical access to system distribution and transmission lines within organi-</li> </ul>	Y	Y	McCain National Defense Authorization Act (NDAA) c. visitors are escorted where appropriate i.e. where we have secure hardware. d. Individuals have cards/keys they are not left in insecure locations e. we will not be printing images.
<ol> <li>Controlling ingress and egress with physical access control systems, devices, or guards.</li> <li>Maintain physical access audit logs for entry or exit points.</li> <li>Escort visitors, and control visitor activity.</li> <li>Secure keys, combinations, and other physical access devices.</li> <li>Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.</li> <li>O3.10.08 Access Control for Transmission</li> <li>Control physical access to system distribution and transmission lines within organizational facilities.</li> </ol>	Y	Y	McCain National Defense Authorization Act (NDAA) c. visitors are escorted where appropriate i.e. where we have secure hardware. d. Individuals have cards/keys they are not left in insecure locations e. we will not be printing images. DWDM, secure routers are in card controlled room (summit contract
<ul> <li>2. Controlling ingress and egress with physical access control systems, devices, or guards.</li> <li>b. Maintain physical access audit logs for entry or exit points.</li> <li>c. Escort visitors, and control visitor activity.</li> <li>d. Secure keys, combinations, and other physical access devices.</li> <li>e. Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.</li> <li>03.10.08 Access Control for Transmission</li> <li>Control physical access to system distribution and transmission lines within organi-</li> </ul>	Y	Y	McCain National Defense Authorization Act (NDAA) c. visitors are escorted where appropriate i.e. where we have secure hardware. d. Individuals have cards/keys they are not left in insecure locations e. we will not be printing images. DWDM, secure routers are in card controlled room (summit contract
<ol> <li>Controlling ingress and egress with physical access control systems, devices, or guards.</li> <li>Maintain physical access audit logs for entry or exit points.</li> <li>Escort visitors, and control visitor activity.</li> <li>Secure keys, combinations, and other physical access devices.</li> <li>Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.</li> <li>O3.10.08 Access Control for Transmission</li> <li>Control physical access to system distribution and transmission lines within organizational facilities.</li> </ol>	Y	Y Y	<ul> <li>c. visitors are escorted where appropriate i.e. where we have secure hardware.</li> <li>d. Individuals have cards/keys they are not left in insecure locations.</li> <li>e. we will not be printing images.</li> </ul>
<ol> <li>Controlling ingress and egress with physical access control systems, devices, or guards.</li> <li>Maintain physical access audit logs for entry or exit points.</li> <li>Escort visitors, and control visitor activity.</li> <li>Secure keys, combinations, and other physical access devices.</li> <li>Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.</li> <li>03.10.08 Access Control for Transmission</li> <li>Control physical access to system distribution and transmission lines within organizational facilities.</li> <li>3.11 RISK ASSESSMENT</li> </ol>			McCain National Defense Authorization Act (NDAA)         c. visitors are escorted where appropriate i.e. where we have secure hardware.         d. Individuals have cards/keys they are not left in insecure locations.         e. we will not be printing images.         DWDM, secure routers are in card controlled room (summit contract pending)         This is part of our regular risk assessment process but we also look in
<ol> <li>Controlling ingress and egress with physical access control systems, devices, or guards.</li> <li>Maintain physical access audit logs for entry or exit points.</li> <li>Escort visitors, and control visitor activity.</li> <li>Secure keys, combinations, and other physical access devices.</li> <li>Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.</li> <li>O3.10.08 Access Control for Transmission Control physical access to system distribution and transmission lines within organizational facilities.</li> <li>3.11 RISK ASSESSMENT</li> <li>O3.11.01 Risk Assessment</li> </ol>			McCain National Defense Authorization Act (NDAA) c. visitors are escorted where appropriate i.e. where we have secure hardware. d. Individuals have cards/keys they are not left in insecure locations. e. we will not be printing images. DWDM, secure routers are in card controlled room (summit contract pending)



03.11.02 Vulnerability Monitoring and Scanning	Y	Y	a. We monitor constantly also conduct third party contract PEN test-
a. Monitor and scan the system for vulnerabilities [Assignment: organization- defined frequency] and when new vulnerabilities affecting the system are identified.			ing b. We patch for vulnerabilities within 24 hours.
b. Remediate system vulnerabilities within [Assignment: organization-defined re- sponse times].			c. third part applications are used for scanning
c. Update system vulnerabilities to be scanned [Assignment: organization-defined			
frequency] and when new vulnerabilities are identified and reported.			
03.11.03 Withdrawn	W		
03.11.04 Risk Response	Y	Y	We respond immediately to any security issue. It receives top prior-
Respond to findings from security assessments, monitoring, and audits. 3.12 SECURITY ASSESSMENT			ity.
03.12.01 Security Assessment	Y	Y	Annual reviews
Assess the security requirements for the system and its environment of operation			
[Assignment: organization-defined frequency] to determine if the requirements have			
been satisfied.			
03.12.02 Plan of Action and Milestones	Y	Y	We use Jira ticketing for all work including security patches and im-
a. Develop a plan of action and milestones for the system:			provements.
1. To document the planned remediation actions to correct weaknesses or deficien- cies noted during security assessments and			
2. To reduce or eliminate known system vulnerabilities.			
b. Update the existing plan of action and milestones based on the findings from:			
1. Security assessments,			
2. Audits or reviews, and			
3. Continuous monitoring activities.			
03.12.03 Continuous Monitoring	Y	Y	Rubin is a mature organization with regular review and monitoring
Develop and implement a system-level continuous monitoring strategy that includes			of all activities including cyber.
ongoing monitoring and security assessments.	14/		Withdraw in revision 2
03.12.04 Withdrawn 03.12.05 Information Exchange	W Y	Y	Withdrawn in revision 3 This is entirely governed by DMTN-199 and its change control pro-
a. Approve and manage the exchange of CUI between the system and other sys-	T		cess.
tems using [Selection (one or more): interconnection security agreements; informa-			
tion exchange security agreements; memoranda of understanding or agreement;			
service-level agreements; user agreements; non-disclosure agreements; other types			
of agreements].			
b. Document interface characteristics, security requirements, and responsibilities for			
each system as part of the exchange agreements.			
c. Review and update the exchange agreements [Assignment: organization-defined frequency].			
3.13 SYSTEM AND COMMUNICATIONS PROTECTION			
03.13.01 Boundary Protection	Y	Y	a. We have border scanning devices.
a. Monitor and control communications at external managed interfaces to the system			b. We use vlans and multiple VPNs to segment the network.
and key internal managed interfaces within the system.			c. Bastions are used where needed and 2FA VPN for all users to
b. Implement subnetworks for publicly accessible system components that are phys-			connect to pixel zone.
ically or logically separated from internal networks.			
c. Connect to external systems only through managed interfaces that consist of			
boundary protection devices arranged in accordance with an organizational security architecture.			
03.13.02 Withdrawn	W		Withdrawn in revision 3
03.13.03 Withdrawn	W		Withdrawn in revision 3
03.13.04 Information in Shared System Resources	Y	Y	DMTN-286 and SITCOMTN-076 cover ground rules on this
Prevent unauthorized and unintended information transfer via shared system re-			
sources.			
03.13.05 Withdrawn	W		
03.13.06 Network Communications – Deny by Default – Allow by Exception	Y	Y	Routing and whitelisting is quite explicit.
Deny network communications traffic by default, and allow network communications			
traffic by exception. 03.13.07 Withdrawn	+		Withdrawn in revision 3
03.13.07 Withdrawn 03.13.08 Transmission and Storage Confidentiality	Y	Y	IPSec and encryption at rest. 2FA VPN to access summit.
Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI		'	
during transmission and while in storage.			
03.13.09 Network Disconnect	Y	Y	We terminate connections after 24 hours
Terminate the network connection associated with a communications session at the			
end of the session or after [Assignment: organization-defined time period] of inactiv-			
ity.			
03.13.10 Cryptographic Key Establishment and Management	Y	Y	
Establish and manage cryptographic keys in the system in accordance with the fol-			
lowing key management requirements: [Assignment: organization-defined require-			
ments for key generation, distribution, storage, access, and destruction].			



		1	
03.13.11 Cryptographic Protection	Y	Y	Disk encryption OS level and AES-256 on the wire.
Implement the following types of cryptography to protect the confidentiality of CUI:			
[Assignment: organization-defined types of cryptography].			
03.13.12 Collaborative Computing Devices and Applications	Y	Y	This is our policy.
a. Prohibit the remote activation of collaborative computing devices and applications			
with the following exceptions: [Assignment: organization-defined exceptions where			
remote activation is to be allowed].			
b. Provide an explicit indication of use to users physically present at the devices.			
03.13.13 Mobile Code	Y	Y	Currently we have no mobile code
a. Define acceptable mobile code and mobile code technologies.			
b. Authorize, monitor, and control the use of mobile code.			
03.13.14 Withdrawn	W		Withdrawn in revision 3
03.13.15 Session Authenticity	Y	Y	VPN and SSL/HTTPS connections are always used.
	T	I I	VFN and SSL/HTTFS connections are always used.
Protect the authenticity of communications sessions.			
03.13.16 Withdrawn	W		Withdrawn in revision 3
3.14 SYSTEM AND INFORMATION INTEGRITY			
03.14.01 Flaw Remediation	Y	Y	Critical vulnerabilities are dealt with within 24 hours.
<ul> <li>a. Identify, report, and correct system flaws.</li> </ul>			
b. Install security-relevant software and firmware updates within [Assignment:			
organization-defined time period] of the release of the updates.			
03.14.02 Malicious Code Protection	Y	Y	
a. Implement malicious code protection mechanisms at system entry and exit points			
to detect and eradicate malicious code.			
b. Update malicious code protection mechanisms as new releases are available in			
accordance with configuration management policies and procedures.			
c. Configure malicious code protection mechanisms to:			
1. Perform scans of the system [Assignment: organization-defined frequency] and			
real-time scans of files from external sources at endpoints or system entry and exit			
points as the files are downloaded, opened, or executed; and			
2. Block malicious code, quarantine malicious code, or take other mitigation actions			
in response to malicious code detection.			
03.14.03 Security Alerts, Advisories, and Directives	Y	Y	Handled by the ISO
a. Receive system security alerts, advisories, and directives from external organiza-			
tions on an ongoing basis.			
b. Generate and disseminate internal system security alerts, advisories, and direc-			
tives, as necessary.			
03.14.04 Withdrawn	W		Withdrawn in revision 3
03.14.05 Withdrawn	W		Withdrawn in revision 3
03.14.06 System Monitoring	Y	Y	Observability system
a. Monitor the system to detect:			
1. Attacks and indicators of potential attacks and			
2. Unauthorized connections.			
b. Identify unauthorized use of the system.			
c. Monitor inbound and outbound communications traffic to detect unusual or unau-			
thorized activities or conditions.			
03.14.07 Withdrawn	W		Withdrawn in revision 3
	Y	Y	
03.14.08 Information Management and Retention	T	<sup>T</sup>	DMTN-199 is the only applicable source.
Manage and retain CUI within the system and CUI output from the system in accor-			
dance with applicable laws, Executive Orders, directives, regulations, policies, stan-			
dards, guidelines, and operational requirements.	L		
3.15. Planning			
03.15.01 Policy and Procedures	Y	Y	
a. Develop, document, and disseminate to organizational personnel or roles the poli-			
cies and procedures needed to satisfy the security requirements for the protection of			
cles and procedures needed to satisfy the security requirements for the protection of		1	
CUI.			



D3152 System Security Plan       Y       A. B. The B2         Decine programs exclured gal nature.       Discrete and text and naturally       C. Initia is considered a public document.         Decine programs       Decine system is exclured to the organization:       C. Initia is considered a public document.         Decines programs       Decines is exclured registering the act of consents to the organization:       C. Initia is considered a public document.         Decines programs       Decines programs       Decines programs       C. Initia is considered a public document.         Decines programs       Decines programs       Decines programs       Decines programs       Decines programs         Decines programs       Decines programs       Decines programs       Decines programs       Decines programs         Decines programs       Decines programs       Decines programs       Decines programs       Decines programs         Decines programs       Decines programs       Decines programs       Decines programs       Decines programs         Decines programs       Decines programs       Decines programs       <				
<ul> <li>Define the constructure system components:</li> <li>Define the constructure system components:</li> <li>Description the optication invest more system that are of concern to the optication:</li> <li>Description the optication invest more system contexponents:</li> <li>Description the optication invest more system contexponentsystem contexponents:</li> <li>Description the option syste</li></ul>	03.15.02 System Security Plan	Y	Y	a. RTN-082
<ul> <li>Define the constructure system components:</li> <li>Define the constructure system components:</li> <li>Description the optication invest more system that are of concern to the optication:</li> <li>Description the optication invest more system contexponents:</li> <li>Description the optication invest more system contexponentsystem contexponents:</li> <li>Description the option syste</li></ul>	a. Develop a system security plan that:			b. review at least annually
1. Under the information topse processed, stored, and variantited by the system Obscribts approximation thrones that up of concerns the originations or connections to inclusive information to the system and any dependencies on connections to inclusive information components is included scheme information components is the system and any dependencies on includes scheme information regimes for metal by escurity regular metals. <ul> <li>Needles individuals that fulfill system roles and responsibilities and includes scheme information regimes for metals or information defined integration.</li> <li>Needles individuals that fulfill system roles and responsibilities and includes scheme information regimes in metals or information defined integration.</li> <li>Needle scheme information regimes in metals append the builties on any dependencies.</li> </ul> <ul> <li>Needle scheme information regimes information information information defined integration.</li> <li>Needle new AUP</li> <li>Need new AUP</li> <li>Needle new AU</li></ul>				-
<ul> <li>B. Bersche specific threads to the system that are of concern to the organization: <ul> <li>D. Surches the organization components:</li> <li>D. Provides an over-even of the system; quartenents for the system and updenetdenes on concern the system or system components:</li> <li>D. Berkew and update the system sceness and reported binks and the system; constrained information concessary for the protection of CLI.</li> <li>D. Berkew and update the system sceness and reported binks and the system; constrained and the system and update the system sceness of the protection of CLI.</li> <li>D. Receive and update the system sceness of the system;</li> <li>Protect the system scenary plan from unauthorized disclosure.</li> <li>P. Protect the system scenary plan from unauthorized disclosure.</li> <li>P. Protect the system scenary plan from unauthorized disclosure.</li> <li>P. Protect the system scenary plan from unauthorized disclosure.</li> <li>P. Protect the system scenary plan from unauthorized disclosure.</li> <li>P. Protect and scenarios the system.</li> <li>Receives addition of the system and system components.</li> <li>Repaire system scontrain estations as the system.</li> <li>Repaire system scontrain estations as the system.</li> <li>Repaire system components.</li> <li>Repaire system components.</li> <li>Repaire system components.</li> <li>Resp</li></ul></li></ul>				
4. Describe the operational environment for the system of any depredencies on connections to other systems or system components:       Image: Components of the security requirements for the system;       Image: Components of the security requirements for the system;       Image: Components of the system security plan (Passignment: organization-defined requency).       Image: Components of the system security plan (Passignment: organization-defined requency).       Image: Components of the system security plan (Passignment: organization-defined requency).       Image: Components of the system security plan (Passignment: organization-defined requency).       Image: Components of the system security plan (Passignment: organization-defined requency).       Image: Components of the system security requirements: organization-defined requency).       Image: Components of the system security requirements of the system.       Image: Components of the system security requirements: organization-defined requency).       Image: Components of the system security requirements: organization-defined requency).       Image: Components of the system security requirements: organization-defined requency).       Image: Components of the system security requirements: organization-defined requency).       Image: Components of the system security requirements: organization-defined requency).       Image: Components of the system security requirements: organization-defined requency).       Image: Components of the components is no longer available for the system security requirements: longer available requency.       Image: Components of the components is no longer available requency.       Image: Components of the components is no longer available requency.       Image: Components of the componenents is no longer available requency.				
or connections to other system components: 5. Provides an overwork of the scurry equirements of the system; 6. Decides the subguards that hill group equirements of the system; 7. Identifies other release in formation machine that discourse. 5. Network and protecting CU. 5. Subside the system security plan function of the protection of CU. 5. Subside the system security plan functions: 6. Protect the system security plan functions: 6. Decides and protecting CU. 5. Subside of behavior 6. Subside the system security plan functions: 6. Releve and update the rules of behavior fastignment: organization-defined fine cuerosis. 6. Releve and update the rules of behavior fastignment: organization-defined fine functions: 6. Releve and update the rules of behavior fastignment: organization-defined fine functions: 6. Releve system security relevence functions: 6. Relevence Anguardistic 10. Subside functions: 6. Relevence Anguardistic relevence Anguardistic 10. Subside functions: 6. Relevence Anguardistic relevence Anguardistic 10. Subside for the system; 7. Relevence Anguardistic relevance Anguardistic relevance Anguardistic 10. Subside for the developer, workey, or manufactures, 8. Relevence Anguardistic relevance Anguardistic relevanc				
9. Products an overwer of the security requirements for the system;       Image: Security Endocutes and responsibilities; and         0. Includies in dividuals that full system roles and responsibilities; and       Image: Security Endocutes the system society pain from number observations of CUU.         0. Structures in individuals that full system roles and responsibilities; and       Image: Security Endocutes the system society pain from number observations of CUU.         0. Structures individuals that full system roles and responsibilities; and the system society pain from number observations of control system.       Products and system society pain from number observations of the system.         0. Receive a document docutes observation of the system.       Receive a document from individuals indicating that they have read, understand, and agree to abole by the roles of behavior foors and system from individual indicating that they have read, understand, and agree to abole by the roles of behavior foors and system components: the components in the components in the components.       Y       Y       Y       Sec INTN-882 Section 2.15         0. Stock of the system and system components: Resignment: organization define frequency in genering principles.       Y       Y       Y       Sec INTN-882 Section 2.15         0. Stock of the system and system components: Resignment: organization define frequency in genering principles.       Y       Y       Y       Sec INTN-882 Section 2.15         0. Stock of the system and system components: Resignment: organization define security requirements;       Resystem and system components: Resignment organ				
c. Describes the singlaucia in place or planned for meeting the security requirements:       Identifies individuals that hull system moles and responsibilities and         1. Induces other release information meessay for the protection of CUL.       Review and updates the system security plan from unauthorized disdosure.       Image: Comparison of the system security plan from unauthorized disdosure.       Image: Comparison of the system security plan from unauthorized disdosure.       Image: Comparison of the system security plan from unauthorized disdosure.       Image: Comparison of the system security plan from unauthorized disdosure.       Image: Comparison of the system security plan from unauthorized disdosure.       Image: Comparison of the system security plan from unauthorized disdosure.       Image: Comparison of the system security plan from unauthorized disdosure.       Image: Comparison of the system security plan from unauthorized disdosure.       Image: Comparison of the system security engineering principles to the development or unauthorized disdosure.       Image: Comparison of the system security engineering principles to the development or unauthorized disdosure.       Image: Comparison of the system security engineering principles to the development or unauthorized disdosure.       Image: Comparison of the system security engineering principles to the development or unauthorized disdosure.       Image: Comparison of the system security engineering principles to the development or unauthorized disdosure.       Image: Comparison of the system security engineering principles to the system security engineering princ	or connections to other systems or system components;			
Inertici         Network         <	<ol><li>Provides an overview of the security requirements for the system;</li></ol>			
Inertici         Network         <	6. Describes the safeguards in place or planned for meeting the security require-			
1. Includes during the index during the measure of the protection of CUL.       Includes during the index during during the index during during the index during duri				
B. Includes other relevant information necessary for the protection of CUL       D. Review and update the system security plan frison unauthorized disclosure.       P       V       Need new AUP         D. Stabilish of Behavior       D. Stabilish of Behavior       P       V       Need new AUP         D. Stabilish of Behavior       D. Stabilish of Behavior       P       V       Need new AUP         D. Stabilish of Behavior       D. Stabilish of Behavior       P       V       Need new AUP         Construction of activative/generation model activative/generation fram induction plant behavior before authorizing curves.       P       V       Need new AUP         Construction of activative/generation model activative/generation model activative/generation framing structures of behavior before authorizing curves.       V       V       See RTN-022 Section 2.15         Stabilish need control activative/generation model activative/generation framing structures of phavior before authorizing curves.       V       V       V       See RTN-022 Section 2.15         Stabilish need control activative/generation framing structures of phavior before authorizing curves.       V       V       V       Week exploitation activative structure structure structure structure and activative structure regioneration.         Stabilish need control activative/generation structure structure structure and activative structure str				
b. Review and update the system security plan from unauthorized disclosure. c. Protect the system security plan from unauthorized disclosure. S1553 Bitles of Behavior a. Estabilish rules that describe the responsibilities and expected behavior for system asge and protecting CU. b. Provide rules to individually who require access to the system. C. Receive a dout rules to individually who require access to the system. C. Receive a dout rules to individually indicating that they have reads. Inderstand, and agree to abube by the rules of behavior bors authorizing as so CL and Services Arguingement from individual indicating that they have reads. Inderstand, and agree to abube by the rules of behavior borsen as so CL and Services Arguingement from individual indicating that they have reads. Inderstand, and agree to abube by the rules of behavior borsen as so CL and Services Arguing Principles 15. System and Services Arguing Principles 15. System and System Components (In Systemment: organization defined fre- thered systems security segmenting introples). 16. Stable The intermine principles 16. System and system Components (In Systemment: organization defined re- tend systems security segmenting introples). 16. System and System Components (In Systemment: organization defined re- tend systems security segmenting introples). 16. Stable Therman defined the system. 16. Stable Therman defined the system Components in no longer availa- able from the developer, word, or manufacturer. 16. Provide options frait fingation or elemanity segment providers are used for sensitive information. 17. Stappi Chain Risk Management Plan 18. Reveive and disposal of the system, system components, or system services. 18. Reveive and disposal of the system, system components, or system services. 18. Reveive and disposal o				
If requency,       Protect the system security plan from unauthorized diclosure.       P       Y       Need new AUP         C31.53 Rules of Behavior       B       P       Y       Need new AUP         C3.53 Rules of Behavior       B       P       Y       Need new AUP         C3.53 Rules of Behavior       B       P       Y       Need new AUP         C3.53 Rules of Behavior       B       P       Y       Need new AUP         C3.53 Rules of Behavior       B       P       Y       Need new AUP         C3.53 Rules of Individuals Noterquire access to the system.       C. Review and update the rules of behavior flasgingment: cognitization-defined fre- caercy, diagother to the system and system security engineering principles to the development or medi system components that another support for the components is no longer anil able from the development system security engineering.       Y       Y       Y       See RTN-0R2 Section 2.15         C3.162 Ursengating System Security engineering principles to the processing storage, or transmission of CUI to complex with the following security requirements; Lissign metric cognization failed security requirements; Lissign metric cognization failed security requirements; Lissign metric cognization failed security requirements; Lissign metric cognization of the system system components, signamet cognisatistoned splatem exp				
c. Proset: the system security plan from unattorized dicclosure.				
0.13.53 Biles of Behavior       P       Y       Need new AUP         Latabils in vice and protecting CU.       D. Provide rules that describe the responsibilities and expected behavior for system       P       Y       Need new AUP         Latabils in vice and protecting CU.       D. Provide rules that describe the responsibilities and expected behavior for system       P       Y       Need new AUP         Latabils in vice and and agree to ability by the rules of behavior bafere authoring access to CU and the system.       C. Review and update the rules of behavior bafere authoring access to CU and the system.       Y       Y       See RTN-882 Section 2.15         B.16.5 System and Services Acquisition       Y       Y       See RTN-882 Section 2.15       Provide place system security engineering principles to the development on modification of the system and system components. Lasgyment: coganization-defined system security engineering principles.       Y       Y       We keep uptodate and licensed.         Log Roude potors for risk mitigation or aliarnative sources for continued support for unsupported components that cannot be replaced.       Y       Y       A. No external providors are used for sensitive information.         A. Require the processes, matchice requirements.       Lasgreen developments that cannot be replaced.       N       N       N       N       N       N       N       N       N       N       N       N       N       N       N       N	frequency].			
a. Establish nelse that describe the responsibilities and expected behavior for system usage and protecting CUI. B. Provide rules to individuals who require access to the system. C. Receive adcumented acknowledgement from individuals indicating that they have read. understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system. G. Review and update the rules of behavior forsignment: organization-defined fre- quercy). 31.6. System and Services Acquisition G. Stopies security engineering principles Apply the following system security engineering principles to the development or find system security engineering principles. Apply the following system security engineering principles. Apply the following system security engineering principles. Apply the following system security engineering principles. B. Requite proteoments the components is no longer awil- before the developer. vend, or or anturbative sources for continued support for transported Components the requirements. B. Requite the providers of external system services used for the processing, storage or transmission of CUI to comply with the following security requirements. Lessing the and document user relax and responsibilities with regard to external system complication of the main dynamic security requirements. Lessing the main developer work or external system services used for the processing, storage or transmission of CUI to comply with the following security requirements. Lessing the main developer work or external system services used for the processing storage or disposed relax security engineering principles. B. Define and document user relax and responsibilities with regard to external system complication for transmitter accel and schemester provides. B. Review and update the supply chain risk management plan [Assignment complication for managing supply chain risk management plan [Assignment complication for managing supply chain risk management plan [Assignment regaration -def	<li>c. Protect the system security plan from unauthorized disclosure.</li>			
a. Establish nelse that describe the responsibilities and expected behavior for system usage and protecting CUI. B. Provide rules to individuals who require access to the system. C. Receive adcumented acknowledgement from individuals indicating that they have read. understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system. G. Review and update the rules of behavior forsignment: organization-defined fre- quercy). 31.6. System and Services Acquisition G. Stopies security engineering principles Apply the following system security engineering principles to the development or find system security engineering principles. Apply the following system security engineering principles. Apply the following system security engineering principles. Apply the following system security engineering principles. B. Requite proteoments the components is no longer awil- before the developer. vend, or or anturbative sources for continued support for transported Components the requirements. B. Requite the providers of external system services used for the processing, storage or transmission of CUI to comply with the following security requirements. Lessing the and document user relax and responsibilities with regard to external system complication of the main dynamic security requirements. Lessing the main developer work or external system services used for the processing, storage or transmission of CUI to comply with the following security requirements. Lessing the main developer work or external system services used for the processing storage or disposed relax security engineering principles. B. Define and document user relax and responsibilities with regard to external system complication for transmitter accel and schemester provides. B. Review and update the supply chain risk management plan [Assignment complication for managing supply chain risk management plan [Assignment complication for managing supply chain risk management plan [Assignment regaration -def	03.15.03 Rules of Behavior	Р	Y	Need new AUP
isage and protecting CUI. b. Provide rules in individuals who require access to the system. c. Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abile by the rules of behavior before authrizing access to CUI and the system. d. Review and update the rules of behavior (Assignment: organization-defined fre- reuerory). 31.6. System and Services Acquition G3.16.0 System services Acquition G3.16.0 System individuals indicating that they have read systems security engineering principles A Replace system components. Kussignment: organization-defined fre- ded systems security engineering principles to the development or modification of the system components. Kussignment: organization- defined systems security engineering principles A Replace system Components is no longer avail- able from the developer, wordor, or manufacturer. b. Provide options for isk mitgation or alternative sources for continued support for unsupported Components that cannot be replaced. G3.16.0 Stetemal System Services used for the processing, storage, retransmission of CUI to comply with the following sequences for continued support for services, including shared responsibilities with regard to external system services, including shared responsibilities with regard to external system services, including shared responsibilities with the grant to external system services, including shared responsibilities with the grant to external system services, including shared responsibilities with regard to external system services,				
b. Provide rules to individuals who require access to the system. c. Receive adouncented acknowleggement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior hefore authorizing access to CI and the system. c. Receive adouncented acknowleggement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior forsing matching matching matching matching matching matching.   316. System and Services Acquisition V V   316. System ind Services Acquisition V V   Apply the following systems security engineering principles to the development or moniforation of the system. V V   Apply the following systems security engineering principles. V V   316. Sizeurity begineering principles. V V   a. Replace system components when support for the components is no longer available from the development or nor main forurer. V V   a. Replace system security engineering principles. V V W   b. Provide options for rink mutgation or alternative sources for continued support for unsupport dor components is no longer available form the development or nor main forurer. N a. No external providers are used for sensitive information.   a. Reguice the providers of external system services. N a. No external providers are used for sensitive information.   a. Support Chin fisk Management Plan associated with the research and development, or support thin fisk management plan form unauthorized discoure. N N   a. Develop and indepeed from striks associated with the research and development, degan, manufacturing, acquisition, delivery, integratins envi				
c. Receive a document da achoovie/gement from individuals indicating that they have read, understand, and agree to able by the rules of behavior lefore authorizing access to CUI and the system. d. Review and update the rules of behavior (Assignment: organization-defined fre- quency). 316. System and Services Acquisition 316. System and Services Acquisition 316. System and Services Acquisition 316. System and Services Acquisition 316. System services principles: 316. System components: (Assignment: organization-defined fre- developy: the following system; security engineering principles to the development or modification of the system components: (Assignment: organization-defined fre- develops: the system components when support for the components is no longer avail- able from the developer, vendor, or manufacturer. b. Provide gottom for risk mitgation or atternative sources for continued support for unsupported components that cannot be replaced. 316.30.316.03.5ternation of the system services cancel for the processing, storage, ret ransmission of CUI to comply with the following cancel reporting: (Assignment companies by esternal system services, and cherniques to monitor security requirements; b. Species and deposition for sensitive information. 317.5.Supply Chain Risk Management Plan 317.5.Supply Chain Risk Management Plan 317.5.Supply Chain Risk Management Plan 317.2.Supply Chain Risk Management plan from unauthorized diclosure. b. Review and udgate the supply chain risk associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, sintenance, and diposal of the system, system components, or system services, b. Review and udgate the supply chain risk associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, sintenance, and diposal of the system, system components, or system services, b. Review and udgate the supply chain risk asociated with the research and development,				
read, understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system. d. Review and update the rules of behavior (Assignment: organization-defined fre- curcory). 31.6. System and Services Acquisition 31.6. System informing informing informing infoldies to the development or application of exystem and system components (Sasignment: organization-defined fre- fined systems ascurity engineering principles. 31.6. System and Services Acquisition 31.6. System and Services Acquisition or alternative (Sasignment: organization-defined fined system security engineering principles. 31.6. System components the system and system components (Sasignment: organization- defined system components when support for the components is no longer avail- able from the developer, vendor, or manufacturer a. Repaice system components the replaced. 31.6. Stransmission of CUI to comply with the following security requirements: (Assign- ment: organization defined security requirements). b. Define and document user roles and responsibilities with regard to external system external. System security engineering principles to monitor security requirements; (Assign- ment: organization defined security requirements; (Assign- ment: organization defined security engineering). b. Define and document user roles and responsibilities with regard to external system security requirements; (Assign- ent torganization defined security). c. Protect and system system. System assice providers of and advalagement. Baking segment plan in take associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, anternature, addisposi of the system, system components, or system services. b. Review and update the spipity chain risk management plan from unauthorized disclosure. 0.17.02 Acquisition strategies, contract tools, and procurement there supply chain risk management plan from unauthorized disclosure. 0.17.02 Acquisition strategies, contract too	<li>b. Provide rules to individuals who require access to the system.</li>			
access to CUI and the system. 4. Review and update the rules of behavior (Assignment: organization defined fre- querry). 316. System and Services Acquisition 316. System and Services Acquisition 316. System and Services Acquisition 316. System Services Acquisition and system security engineering principles to the development or modification of the system components: (Assignment: organization-defined system security engineering principles). 316. System components when support for the components is no longer avail- bef from the developmer, weld, or mandicature: b. Provide options for risk milgation or alternative sources for continued support for an Replace system components when support for the components is no longer avail- bef from the developmer, weld, or mandicature: b. Provide options for risk milgation or alternative sources for continued support for the anyotices of setternative sources for continued support for anyotice the providers of a setternative sources for continued support for the anyotices in during shared responsibilities with tergard to external system settings, manufacturing, acquisition, delevelopments, leasing, anyotice the providers on an ongoing basis. 317.5 Supply Chain fisk Management Pian a. Bevelop a pian for managing supply chain risk management pian forsignment: organization defined forcuring, acquisition, delevelopment, experiment and Processes. b. Review and update the supply chain risk management pian forsignment: organization defined for equerendis. b. Review and delement and processes. b. Review and telement and Processes. c. Protect the supply chain risk management pia	c. Receive a documented acknowledgement from individuals indicating that they have			
access to CUI and the system. 4. Review and update the rules of behavior (Assignment: organization defined fre- querry). 316. System and Services Acquisition 316. System and Services Acquisition 316. System and Services Acquisition 316. System Services Acquisition and system security engineering principles to the development or modification of the system components: (Assignment: organization-defined system security engineering principles). 316. System components when support for the components is no longer avail- bef from the developmer, weld, or mandicature: b. Provide options for risk milgation or alternative sources for continued support for an Replace system components when support for the components is no longer avail- bef from the developmer, weld, or mandicature: b. Provide options for risk milgation or alternative sources for continued support for the anyotices of setternative sources for continued support for anyotice the providers of a setternative sources for continued support for the anyotices in during shared responsibilities with tergard to external system settings, manufacturing, acquisition, delevelopments, leasing, anyotice the providers on an ongoing basis. 317.5 Supply Chain fisk Management Pian a. Bevelop a pian for managing supply chain risk management pian forsignment: organization defined forcuring, acquisition, delevelopment, experiment and Processes. b. Review and update the supply chain risk management pian forsignment: organization defined for equerendis. b. Review and delement and processes. b. Review and telement and Processes. c. Protect the supply chain risk management pia	read, understand, and agree to abide by the rules of behavior before authorizing			
i. Review and update the rules of behavior [Assignment: organization-defined fre- ueuroy].       Image: System and Services Acquisition       Image: System and Services Acquisition         31.6.0 Security Engineering Principles       Y       Y       See RTN-082 Section 2.15         Apply the following system security engineering principles to the development or modification of the system components. [Assignment: organization-defined system security engineering principles].       Y       Y       We keep uptodate and licensed.         as Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.       Y       Y       We keep uptodate and licensed.         b. Provide gotion for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.       Y       Y       We keep uptodate and licensed.         a. Regular the providers of external system services. Including shared responsibilities with the grade to external system. Security requirements, [Assign- ment: organization-defined security requirements, [Assign- ment: organization-defined security requirements, [Assign- ment: organization-defined frequency].       N       N       N         13.17.50 Stypering Risk Management Plan a. Develop a plan for managing supply chain risk associated with the research and development, faugh, manufacturing, acquation, delivery, integration, operations, manateance, and disposal of the system, system components or system services.       N       N       N       N       N       Aspalicable for this project.				
outercy].     N     N       315. System and Services Acquisition     V     V       03.16.01 Security Engineering Principles     Y     V       Apply the following system scorengoments: (Assignment: organization-defined system scurity engineering principles)     Y     V       03.16.02 Unsupported System Components     Y     V     See RTN-082 Section 2.15       03.16.02 Unsupported System Components     Y     V     We keep uptodate and licensed.       03.16.02 Unsupported System Components     Y     V     We keep uptodate and licensed.       03.16.02 External System Tormanutature:     P     V     We keep uptodate and licensed.       03.16.02 External System Services     P     V     We keep uptodate and licensed.       03.16.02 External System Services     P     V     We keep uptodate and licensed.       03.16.02 External System Services     P     V     We keep uptodate and licensed.       03.16.02 External System Services     P     V     We keep uptodate and licensed.       03.16.02 External System Services     P     V     P     A. No external providors are used for sensitive information.       3.17.05 Supply Chain Risk Management 10     P     N     N     N       03.17.05 Supply Chain Risk Management 10     N     N     N     N       03.17.05 Supply Chain Risk Management 10 <td< td=""><td>-</td><td></td><td></td><td></td></td<>	-			
316. System and Services Acquisition       V       See RTN-082 Section 2.15         Apply the following system security engineering principles to the development or modification of the system and system components: (Assignment: organization-defined systems components when support for the components is no longer available from the developer, vendor, or manufacturer.       Y       Y       We keep uptodate and licensed.         A Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.       Y       Y       We keep uptodate and licensed.         B- Provide options for risk mitaging security requirements; (Assignment: organization-defined requercy).       N         03.17.0 Supply Chain Risk Management Plan       N       N       N       N         03.17.0 Supply Chain Risk Management Plan from unauthorized disclosure.       N       N       N       N       N         03.17.0 Supply Chain Risk management plan from unauthorized disclosure.       N       N       N				
103.16.01 Security Engineering Principles     Y     Y     See RTN-082 Section 2.15       Apply the following systems security engineering principles to the development of fined system security engineering principles.     Y     Y     See RTN-082 Section 2.15       03.16.02 Unsported System Components: Assignment: organization- de- fined system security engineering principles.     Y     Y     We keep uptodate and licensed.       03.16.02 Unsported System Components that components is no longer avail- able from the developer, endor, or manufacture.     Y     Y     We keep uptodate and licensed.       03.16.03 External System services     Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.     Y     Y     a. No external providors are used for sensitive informalton.       0.31.63.2 External System Services     C     Y     Y     a. No external providors are used for sensitive informalton.       a. Require the providers of external system services used for the grant be each system, services, including shared responsibilities with egand to external system services, including fair formanging supply chain risk associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components and roccess.     N     N       03.17.02 Supply Chain Risk Management plan form unsuphrcited disclosure.     N     N     N       03.17.02 Supply Chain Risk Management plan form unsuphrcited disclosure.     N     N     N				
Apply the following system security regineering principles: 0 the development or modification of the system components: [Assignment: organization-defined systems excurity engineering principles].       Y       Y         03.16.02 Unsupported System Components: An explore on the development of the components is no longer available from the developer, vendor, or manufacturer.       Y       Y       We keep uptodate and licensed.         03.16.02 Unsupported System Components that cannot be replaced.       Y       Y       We keep uptodate and licensed.         03.16.03 Eterment System Services       Y       Y       A sequire the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: (Assignment: organization-defined security requirements).       Y       Y       a. No external providors are used for sensitive information.         0.17.01 Supply Chain Risk Management       Image: Component Sing supply Chain Risk Management Plan       N       N       N         0.21.70.01 Supply Chain Risk Management plan form unauthorized discissure.       N       N       N applicable for this project.         0.31.70.3 Supply Chain Risk Management plan form unauthorized discissure.       N       N       N applicable for this project.         0.31.70.3 Supply Chain Risk Management plan form unauthorized discissure.       N       N       N applicable for this project.         0.31.70.3 Supply Chain Risk Management plan form unauthorized discissure.       N				
modification of the system and system components: [Asignment: organization-defined system scurry engineering principles].YY03.16.20 Unsupported System Components the support for the components is no longer available from the developer, vendor, or manufacturer.YYWe keep uptodate and licensed.b. Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.YYYa. Require the provides of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements; [Assignment: organization-defined secure and system services including shared responsibilities with regard to external system services.YY3.17. Supp) Chain Risk Management PlanNNNot applicable for this project.a. Develop and disposid of the system, system servicesNNNa. Transmistion of displate the supply chain risk associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposid of the system, system components and system services.NN3.17. Supply Chain Risk Management PlanNNNNa. Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain riskNNN3.17. Supply Chain Risk management plan form unauthorized disclosure.NNNN3.17. Supply Chain Risk management plan form unauthorized disclosure.NNNN3.17. Supply Chain Risk management plan form unauthorized disclosure.NN		Y	Y	See RTN-082 Section 2.15
modification of the system and system components: [Asignment: organization-defined system scurry engineering principles].YY03.16.20 Unsupported System Components the support for the components is no longer available from the developer, vendor, or manufacturer.YYWe keep uptodate and licensed.b. Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.YYYa. Require the provides of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements; [Assignment: organization-defined secure and system services including shared responsibilities with regard to external system services.YY3.17. Supp) Chain Risk Management PlanNNNot applicable for this project.a. Develop and disposid of the system, system servicesNNNa. Transmistion of displate the supply chain risk associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposid of the system, system components and system services.NN3.17. Supply Chain Risk Management PlanNNNNa. Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain riskNNN3.17. Supply Chain Risk management plan form unauthorized disclosure.NNNN3.17. Supply Chain Risk management plan form unauthorized disclosure.NNNN3.17. Supply Chain Risk management plan form unauthorized disclosure.NN	Apply the following systems security engineering principles to the development or			
Inted systems security engineering principles].       Y       Y       We keep uptodate and licensed.         03.16.02 Unsupported System Components       An equipation or alternative sources for continued support for unsupported components when support for the components is no longer available from the developer, vendor, or manufacturer.       Y       Y       We keep uptodate and licensed.         03.16.03 External System Services       Y       Y       a. Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment organization-defined security requirements].       Y       a. No external providors are used for sensitive information.         0.17.01 Supply Chain Risk Management 10a       N       N       N       Not applicable for this project.         0.2017.01 Supply Chain Risk Management 10a       N       N       N       Not applicable for this project.         0.2017.01 Supply Chain Risk Management 10a       N       N       Not applicable for this project.         0.2017.01 Supply Chain Risk Management 10a       N       N       N       Not applicable for this project.         0.2017.01 Supply Chain Risk Management 10an (Assignment: organization-defined frequery).       Not applicable for this project.       N         0.2017.01 Supply Chain Risk management plan from unauthorized disclosure.       N       N       N         03.17.02 Supply Chain Risk management				
103.16.20 Unsupported System Components       Y       Y       Y       We keep uptodate and licensed.         a. Replace system components when support for the components is no longer available from the developer, whole options for risk mitgation or atternative sources for continued support for unsupported components that cannot be replaced.       Y       Y       We keep uptodate and licensed.         0.8. Require the providers of external system services and components is no longer available.       Y       Y       P       P         a. Require the providers of external system services used for the processing. storage, or transmission of CU to comply with the following security requirements; [Assignment: organization-defined security requirements].       Y       Y       P       P       a. No external providors are used for sensitive information.         0.3.17.01 Supply Chain Risk Management Plan       D       P				
a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.       b. Provide options for risk mitagino or alternative sources for continued support for unsupported components that cannot be replaced.       V       V       a. No external providors are used for sensitive informaiton.         a. Reguire the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements].       V       Y       a. No external providors are used for sensitive informaiton.         b. Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with regard to external system services and techniques to monitor security requirement compliance by external service providers on an ongoing basis.       N		V	V	We keep uptedate and licensed
able from the developer, vendor, or manufacturer.       b. Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.       V       V       a. No external providors are used for sensitive informaiton.         03.16.03 External System Services       V       V       a. No external providors are used for sensitive informaiton.         03.16.03 External System Services       V       V       a. No external providors are used for sensitive informaiton.         03.16.03 External System Services       V       V       A. No external providors are used for sensitive informaiton.         03.16.03 External System Services       V       V       A. No external providors are used for sensitive informaiton.         1. Define and document user roles and responsibilities with external service providers on an origing basis.       V       V       N         1.7. Suppl Chain Risk Management Plan       V       N       N       Not applicable for this project.         0. Pevelop plan for managing suppl vhain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and diposal of the system, system components, or system services.       N       N       Not applicable for this project.         03.17. Suppl Chain Risk Management plan (Tasignities used for sensity engineer plan (Tasignities associated with the research and development, design, manufacturing, acquisition, strategies, contract tools, and procurees. <t< td=""><td></td><td>I I</td><td>T</td><td>we keep uptodate and licensed.</td></t<>		I I	T	we keep uptodate and licensed.
b. Provide options for isk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.     Y     Y       03.16.03 External System Services     A Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assign- ment organization-defined security requirements].     Y     Y       b. Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers.     Y     N     a. No external providors are used for sensitive information.       0. Define and document user roles and responsibilities with external service providers an ongoing basis.     Image: Complex com				
unsupported components that cannot be replaced.       V         03.16.03 External System Services       V         03.16.03 External System Services       V         0. Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment organization-defined security requirements].       V       A. No external providors are used for sensitive information.         b. Define and document user roles and responsibilities with external service providers.       C. Implement brocks, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.       N       N         3.17. Supply Chain Risk Management Plan       N       N       N applicable for this project.         a. Develop a plan for managing supply chain risk associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system components, or system services.       N       N       Not applicable for this project.         b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency].       N       N       Not applicable for this project.         0.317.03 Supply Chain Risk management plan from unauthorized disclosure.       N       N       Not applicable for this project.         0.217.03 Supply Chain risk management plan from unauthorized disclosure.       N       N       Not applicable for this project.	able from the developer, vendor, or manufacturer.			
03.16.03 External System Services       Y       Y       a. No external providors are used for sensitive informaiton.         a. Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements].       Y       Y       a. No external providors are used for sensitive informaiton.         b. Define and document user roles and responsibilities with external service providers.       N       No external service providers on an ongoing basis.         3.17. Supply Chain Risk Management       N       N       Not applicable for this project.         a. Develop a plan for managing supply chain risk management plan form unauthorized disclosure.       N       N       Not applicable for this project.         03.17.01 Supply Chain Risk Management plan from unauthorized disclosure.       N       N       Not applicable for this project.         0.317.01 Supply Chain Risk management plan from unauthorized disclosure.       N       N       N       Not applicable for this project.         0.317.03 Cacquisition Strategies, Tools, and Methods       N       N       N       Not applicable for this project.         03.170.2 Acquisition strategies, tools, and procurement methods to identify, protect against, and mitigate supply chain risks.       N       N       N         03.170.3 Supply Chain Risk management plan from unauthorized disclosure.       N       N	b. Provide options for risk mitigation or alternative sources for continued support for			
03.16.03 External System Services       Y       Y       a. No external providors are used for sensitive informaiton.         a. Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements].       Y       Y       a. No external providors are used for sensitive informaiton.         b. Define and document user roles and responsibilities with external service providers.       N       No external service providers on an ongoing basis.         3.17. Supply Chain Risk Management       N       N       Not applicable for this project.         a. Develop a plan for managing supply chain risk management plan form unauthorized disclosure.       N       N       Not applicable for this project.         03.17.01 Supply Chain Risk Management plan from unauthorized disclosure.       N       N       Not applicable for this project.         0.317.01 Supply Chain Risk management plan from unauthorized disclosure.       N       N       N       Not applicable for this project.         0.317.03 Cacquisition Strategies, Tools, and Methods       N       N       N       Not applicable for this project.         03.170.2 Acquisition strategies, tools, and procurement methods to identify, protect against, and mitigate supply chain risks.       N       N       N         03.170.3 Supply Chain Risk management plan from unauthorized disclosure.       N       N	unsupported components that cannot be replaced.			
a. Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assign- ment: organization-defined security requirements].b. Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers.N0. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.NN03.17. Supply Chain Risk Management Plan a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services.NNNNNNot applicable for this project.03.17. Supply Chain risk management plan from unauthorized disclosure. Organization-defined frequency). c. Protext the supply chain risk management plan form unauthorized disclosure. 03.17.02 Supply Chain risk management plan from unauthorized disclosure. 03.17.02 Supply Chain risk management plan frox supply chain risks.NN03.17.02 Supply Chain risk management plan from unauthorized disclosure. 03.17.02 Supply Chain reguirements and processes b. Enforce the following security requirements to protext against supply chain risks.NN03.17.03 Supply Chain reguirementsNN<		V	v	a. No external providors are used for sensitive information
or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements].Security requirements].Security requirements].b. Define and document user roles and responsibilities with external service providers.Security requirements].Security requirements].3.17. Supply Chain Risk ManagementSecurity requirement is and recompliance by external service providers on an ongoing basis.NN3.17. Supply Chain Risk Management PlanNNNot applicable for this project.3. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services.NN0. Review and update the supply chain risk management plan [Assignment: organization-defined frequency].NNNot applicable for this project.03.17.02 Acquisition Strategies, Tools, and MethodsNNNNot applicable for this project.03.17.03 Supply Chain Requirements and ProcessesNNNN03.17.03 Supply Chain Requirements and ProcessesNNNN03.17.04 Acquisition strategies, roots security requirements or organization-defined security requirements and processesNNN03.17.03 Supply Chain Requirements and Processes <td></td> <td></td> <td>· ·</td> <td>a. No external providors are asea for sensitive information.</td>			· ·	a. No external providors are asea for sensitive information.
ment: organization-defined security requirements]. b. Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers. c. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.NN3.17. Supply Chain Risk Management 03.17.01 Supply Chain Risk Management Plan a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency]. c. Protect the supply chain risk management plan [Assignment: organization defined frequency]. c. Protect the supply chain risk management plan (Assignment: organization strategies, contract tools, and procurement methods to learning and processes. a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain related events: [Assignment: organization-defined events].NNN applicable for this project.03.17.02 Multi networks and processes. b. Enforce the following security requirements to protect against and mitigate supply chain risks to the system, system components, or system services and to limit the harm or con- sequences from supply chain-related events: [Assignment: organization-defined security requirements].NNN applicable for this project.03.17.02 Multi networks to comply with to tal NUSTBOO-171 requirements98Implement acquirementsImplement acquirements03.17.03 Lupply Chain related events: [Assignment: organization-defined se-				
b. Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers.           c. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.       N       N         3.17. Supply Chain Risk Management Plan       N       N       N       N         a. Develop a plan for managing supply chain risk associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services.       N       N       N applicable for this project.         c. Protect the supply chain risk management plan from unauthorized disclosure.       N       N       N       N         03.17.01 Supply chain risk management plan from unauthorized disclosure.       N       N       N       N         03.17.03 Supply chain risk management plan from unauthorized disclosure.       N       N       N       N         03.17.03 Supply chain risk management plan from unauthorized disclosure.       N       N       N       N         03.17.03 Supply chain risk anagement and processes       N       N       N       N       N         a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain related events: [Assignment: organization-defined security requirements].       98				
services, including shared responsibilities with external service providers. c. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.Service providers on an ongoing basis.3.17. Supply Chain Risk ManagementImage of the system system of the system service providers. a. Develop a plan for managing supply chain risk associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. b. Review and update the supply chain risk management plan form unauthorized disclosure.NNN03.17.02 Acquisition Strategies, Tools, and MethodsNNNNot applicable for this project.03.17.03 Supply Chain risk management plan form unauthorized disclosure. or 317.02 Acquisition Strategies, Tools, and mitigate supply chain risks.NNN03.17.03 Supply Chain Requirements and Processes a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain related events: [Assignment: organization-defined security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or con- sequences from supply chain-related events: [Assignment: organization-defined security requirements].NNNTotal Rubin Intends to comply with98Total Rubin Intends to comply with22Total Rubin Intends to comply with2	ment: organization-defined security requirements].			
c. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.Image: service providers on an ongoing basis.3.17. Supply Chain Risk Management Plan a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency]. c. Protect the supply chain risk management plan from unauthorized disclosure.NNNot applicable for this project.03.17.02 Acquisition Strategies, Tools, and Methods Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.NNNot applicable for this project.03.17.03 Supply Chain Requirements and Processes a. Establish a process for identifying and addressing weaknesses or deficiencies in the system, system components, or system services and to limit the harm or con- sequences from supply chain-related events: [Assignment: organization-defined se- currity requirementsNNot applicable for this project.Total NitifeB0-171 requirements98Total Rubin Intends to comply with5Total Rubin Intends to comply with2Total Rubin Intends to comply with2	b. Define and document user roles and responsibilities with regard to external system			
c. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.Image: service providers on an ongoing basis.3.17. Supply Chain Risk Management Plan a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency]. c. Protect the supply chain risk management plan from unauthorized disclosure.NNNot applicable for this project.03.17.02 Acquisition Strategies, Tools, and Methods Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.NNNot applicable for this project.03.17.03 Supply Chain Requirements and Processes a. Establish a process for identifying and addressing weaknesses or deficiencies in the system, system components, or system services and to limit the harm or con- sequences from supply chain-related events: [Assignment: organization-defined se- currity requirementsNNot applicable for this project.Total NitifeB0-171 requirements98Total Rubin Intends to comply with5Total Rubin Intends to comply with2Total Rubin Intends to comply with2	services, including shared responsibilities with external service providers.			
compliance by external service providers on an ongoing basis.Image: compliance by external service providers on an ongoing basis.3.17. Supply Chain Risk ManagementN03.17.01 Supply Chain Risk Management PlanNa. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. b. Review and update the supply chain risk management plan from unauthorized disclosure.NNN03.17.02 Acquisition Strategies, Tools, and MethodsNNNNDevelop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.NNN applicable for this project.03.17.02 Acquisition Strategies, Tools, and MethodsNNN applicable for this project.03.17.02 Acquisition Strategies, roots, and Processes a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain requirements and processes.NNN applicable for this project.03.17.03 ExperimentsSettern system components, or system services and to limit the harm or con- sequences from supply chain-related events: [Assignment: organization-defined se- curity requirementsNNNTotal NUSTB00-171 requirementsSettern setternalSetSetTotal Rubin Intends to comply withSZTotal Rubin Intends to comply withSZTotal Rubin Intends to comply withSZTotal Rubin Intends to comply with <td></td> <td></td> <td></td> <td></td>				
3.17. Supply Chain Risk Management       N       N         03.17.01 Supply Chain Risk Management Plan       N       N         a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services.       N       N       N       Not applicable for this project.         b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency].       C. Protect the supply chain risk management plan from unauthorized disclosure.       N       N       N       Not applicable for this project.         03.17.02 Acquisition Strategies, Tools, and Methods       N       N       N       Not applicable for this project.         03.17.03 Supply Chain risk management plan from unauthorized disclosure.       N       N       N       Not applicable for this project.         03.17.03 Supply Chain Requirements and Processes       N       N       N       Not applicable for this project.         03.17.03 Supply Chain Requirements on Processes       N       N       N       Not applicable for this project.         03.17.03 Supply Chain requirements or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization- defined security requirements].       N       N         03.17.03 Supply Chain-related events: [Assignment: organization- defined security				
03.17.01 Supply Chain Risk Management Plan       N       N       N       N         a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services.       N       N       N       N       N       N       Not applicable for this project.         03.17.01 Supply Chain risk management plan form unauthorized disclosure.       N       N       N       N       Not applicable for this project.         03.17.02 Acquisition Strategies, Tools, and Methods       N       N       N       Not applicable for this project.         03.17.03 Supply Chain requirements and Processes       N       N       N       Not applicable for this project.         03.17.03 Supply Chain Requirements to protect against supply chain risks.       N       N       N       Not applicable for this project.         03.17.03 Supply Chain Requirements and Processes       N       N       N       Not applicable for this project.         04. Explore the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined security requirements].       98         Total NIST800-1711 requirements       98       1         Total Rubin Intends to comply with <td></td> <td>+</td> <td></td> <td></td>		+		
a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. D. Review and update the supply chain risk management plan [Assignment: organization-defined frequency]. c. Protect the supply chain risk management plan from unauthorized disclosure.NN03.17.02 Acquisition Strategies, Tools, and Methods Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.NN03.17.03 Supply Chain Requirements and Processes a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain-related events: [Assignment: organization- defined se- curity requirements].NNTotal NIST800-171 requirements98Total Rubin Intends to comply fully with91Total Rubin Intends to comply with Total Rubin Intends to apartially comply with2		1		
development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency]. c. Protect the supply chain risk management plan from unauthorized disclosure.NNot applicable for this project.03.17.02 Acquisition Strategies, Tools, and Methods Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.NNot applicable for this project.03.17.03 Supply Chain Requirements and Processes a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes. b. Enforce the following security requirements to protect against supply chain risksNNot applicable for this project.03.17.03 Nupply Chain related events: [Assignment: organization- defined security requirements].NNot applicable for this project.03.17.04 Nursteenenets9810 Total Rubin Intends to comply fully with9110 Total Rubin Intends to partially comply with210 Total Rubin Intends to apratally comply with2	03.17.01 Supply Chain Risk Management Plan	N	N	Not applicable for this project.
development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency]. c. Protect the supply chain risk management plan from unauthorized disclosure.NNot applicable for this project.03.17.02 Acquisition Strategies, Tools, and Methods Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.NNot applicable for this project.03.17.03 Supply Chain Requirements and Processes a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes. b. Enforce the following security requirements to protect against supply chain risksNNot applicable for this project.03.17.03 Nupply Chain related events: [Assignment: organization- defined security requirements].NNot applicable for this project.03.17.04 Nursteenenets9810 Total Rubin Intends to comply fully with9110 Total Rubin Intends to partially comply with210 Total Rubin Intends to apratally comply with2	a. Develop a plan for managing supply chain risks associated with the research and			
maintenance, and disposal of the system, system components, or system services. b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency]. c. Protect the supply chain risk management plan from unauthorized disclosure.NNNot applicable for this project.03.17.02 Acquisition Strategies, Tools, and Methods Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.NNNot applicable for this project.03.17.03 Supply Chain Requirements and Processes a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain system components, or system services and to limit the harm or con- sequences from supply chain-related events: [Assignment: organization- defined se- curity requirements].NNNot applicable for this project.Total NIST800-171 requirements Total Rubin Intends to comply with9811Total Rubin Intends to partially comply with Total Rubin Intends to partially comply with51Total Rubin Intends to partially comply with2Total Rubin Intends to partially comply with2				
b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency]. c. Protect the supply chain risk management plan from unauthorized disclosure.Image: Complex with in 2024Not applicable for this project.03.17.03 Supply Chain Requirements and Processes a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes. b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or con- sequences from supply chain-related events: [Assignment: organization- defined security requirements].NNot applicable for this project.Total NIST800-171 requirements Total Rubin Intends to comply withS98Total Rubin Intends to partially comply withSSTotal Rubin Intends to partially comply withSTotal Rubin Intends to partially comply withSState Rubin Intends to partially complex with in 2024S				
organization-defined frequency]. c. Protect the supply chain risk management plan from unauthorized disclosure.NN03.17.02 Acquisition Strategies, Tools, and Methods Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.NN03.17.03 Supply Chain Requirements and Processes a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes. b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or con- sequences from supply chain-related events: [Assignment: organization- defined se- curity requirements].98Total NUST800-171 requirements Total Rubin Intends to comply with5Total Rubin Intends to partially comply with2Total Rubin Intends to partially comply with84				
c. Protect the supply chain risk management plan from unauthorized disclosure.Image: constraint of the supply chain risk management plan from unauthorized disclosure.Image: constraint of the supply chain risk management plan from unauthorized disclosure.03.17.02 Acquisition Strategies, Tools, and Methods Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.NNot applicable for this project.03.17.03 Supply Chain Requirements and Processes a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.NNNot applicable for this project.b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or con- sequences from supply chain-related events: [Assignment: organization- defined se- curity requirements].98Image: constraint of processesTotal NUST800-171 requirements915Total Rubin Intends to comply with5Total Rubin Intends to partially comply with2Total Rubin Intends to partially comply with2				
03.17.02 Acquisition Strategies, Tools, and Methods       N       N       N       Not applicable for this project.         Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.       N       N       Not applicable for this project.         03.17.03 Supply Chain Requirements and Processes       N       N       N       Not applicable for this project.         03.17.03 Supply Chain Requirements and Processes       N       N       N       Not applicable for this project.         a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.       N       N       N         b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization- defined security requirements].       98         Total NIST800-171 requirements       91         Total Rubin Intends to comply with       5         Total Rubin Intends to partially comply with       2         Total Rubin Intends to partially comply with       2         Total Rubin Complies with in 2024       84				
Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.NNot applicable for this project.03.17.03 Supply Chain Requirements and Processes a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes. b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or con- sequences from supply chain-related events: [Assignment: organization- defined se- curity requirements].98Total NIST800-171 requirements91Total Rubin Intends to comply with5Total Rubin Intends to partially comply with2Total Rubin Intends to partially comply with84	c. Protect the supply chain risk management plan from unauthorized disclosure.			
methods to identify, protect against, and mitigate supply chain risks.Image: Constraint of the supply chain Requirements and Processes03.17.03 Supply Chain Requirements and ProcessesNNa. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.NNb. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization- defined security requirements].98Total NIST800-171 requirements91Total Rubin Intends to comply with5Total Rubin Intends to partially comply with2Total Rubin Intends to partially comply with84	03.17.02 Acquisition Strategies, Tools, and Methods	N	N	Not applicable for this project.
methods to identify, protect against, and mitigate supply chain risks.Image: Constraint of the supply chain Requirements and Processes03.17.03 Supply Chain Requirements and ProcessesNNa. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.NNb. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization- defined security requirements].98Total NIST800-171 requirements91Total Rubin Intends to comply with5Total Rubin Intends to partially comply with2Total Rubin Intends to partially comply with84	Develop and implement acquisition strategies, contract tools, and procurement			
03.17.03 Supply Chain Requirements and ProcessesNNNot applicable for this project.a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.NNNot applicable for this project.b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or con- sequences from supply chain-related events: [Assignment: organization- defined se- curity requirements].98Total NIST800-171 requirements91Total Rubin Intends to comply with5Total Rubin Intends to partially comply with2Total Rubin Intends to partially comply with84				
a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes. b. Enforce the following security requirements to protect against supply chain risks to the system components, or system services and to limit the harm or con- sequences from supply chain-related events: [Assignment: organization- defined se- curity requirements].98Total NIST800-171 requirements91Total Rubin Intends to comply with5Total Rubin Intends to comply with2Total Rubin Intends to partially comply with2		N	N	Not applicable for this project
the supply chain elements and processes.b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or con- sequences from supply chain-related events: [Assignment: organization- defined se- curity requirements].98Total NIST800-171 requirements98Total Rubin Intends to comply fully with91Total Rubin Intends to comply with5Total Rubin Intends to partially comply with2Total Rubin Intends to partially comply with84		IN		Not applicable for this project.
b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or con- sequences from supply chain-related events: [Assignment: organization- defined se- curity requirements].98Total NIST800-171 requirements98Total Rubin Intends to comply with91Total Rubin Intends to partially comply with5Total Rubin Intends to partially comply with2Total Rubin Intends to partially comply with84				
to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization- defined security requirements].98Total NIST800-171 requirements98Total Rubin Intends to comply fully with91Total Rubin Intends not to comply with5Total Rubin Intends to partially comply with2Total Rubin Intends to partially comply with84				
sequences from supply chain-related events: [Assignment: organization- defined se- curity requirements].98Total NIST800-171 requirements98Total Rubin Intends to comply fully with91Total Rubin Intends not to comply with5Total Rubin Intends to partially comply with2Total Rubin Intends to partially comply with84	b. Enforce the following security requirements to protect against supply chain risks			
sequences from supply chain-related events: [Assignment: organization- defined se- curity requirements].98Total NIST800-171 requirements98Total Rubin Intends to comply fully with91Total Rubin Intends not to comply with5Total Rubin Intends to partially comply with2Total Rubin Intends to partially comply with84	to the system, system components, or system services and to limit the harm or con-			
curity requirements].98Total NIST800-171 requirements98Total Rubin Intends to comply fully with91Total Rubin Intends not to comply with5Total Rubin Intends to partially comply with2Total Rubin Complies with in 202484				
Total NIST800-171 requirements98Total Rubin Intends to comply fully with91Total Rubin Intends not to comply with5Total Rubin Intends to partially comply with2Total Rubin Complies with in 202484				
Total Rubin Intends to comply fully with91Total Rubin Intends not to comply with5Total Rubin Intends to partially comply with2Total Rubin Complies with in 202484		+		
Total Rubin Intends not to comply with     5       Total Rubin Intends to partially comply with     2       Total Rubin Complies with in 2024     84	-	1		
Total Rubin Intends to partially comply with     2       Total Rubin Complies with in 2024     84	Total Rubin Intends to comply fully with		91	
Total Rubin Intends to partially comply with     2       Total Rubin Complies with in 2024     84	Total Rubin Intends not to comply with		5	
Total Rubin Complies with in 2024     84		1		
		+		
I otal kupin Partially Complies with in 2024 4	· · · ·	+		
	Total Rubin Partially Complies with in 2024		4	



### **B** References

[SQR-041], Allbery, R., 2022, Science Platform security risk assessment, URL https://sqr-041. lsst.io/,

Vera C. Rubin Observatory SQuaRE Technical Note SQR-041

- [SITCOMTN-076], Bechtol, K., on behalf of the Rubin Observatory Project Science Team, S.R., 2024, Information Sharing during Commissioning, URL https://sitcomtn-076.lsst.io/, Vera C. Rubin Observatory Commissioning Technical Note SITCOMTN-076
- [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
- [RTN-073], Dubois, R., 2024, Rules of Engagement for Accessing Data During the Embargo Period, URL https://rtn-073.lsst.io/, Vera C. Rubin Observatory Technical Note RTN-073
- [RTN-072], Guy, L., 2024, Rubin Operations Change Control Process, URL https://rtn-072. lsst.io/, Vera C. Rubin Observatory Technical Note RTN-072
- [ACP], Marshall, P., 2024, Access Control Plan for the Vera C. Rubin Observatory U.S. Data Facility Embargo Rack , URL https://ls.st/ACP, Internal document
- [DMTN-286], O'Mullane, W., Economou, F., 2024, Data security for Rubin communication channels, URL https://dmtn-286.lsst.io/, Vera C. Rubin Observatory Data Management Technical Note DMTN-286
- [DMTN-199], O'Mullane, W., Allbery, R., AlSayyad, Y., et al., 2023, Rubin Observatory Data Security Standards Implementation, URL https://dmtn-199.lsst.io/, Vera C. Rubin Observatory Data Management Technical Note DMTN-199
- [RTN-030], O'Mullane, W., Allbery, R., Dubois, R., Lim, K., 2024, Rubin Data and Information Security Plan, URL https://rtn-030.lsst.io/, Vera C. Rubin Observatory Technical Note RTN-030



- [RDO-71], Roberts, A., Blum, R., Claver, C., et al., 2024, Rubin Observatory Risk and Opportunity Management Plan, URL https://rdo-71.lsst.io/, Vera C. Rubin Observatory RDO-71
- [NIST.SP.800-171r3], Ross, R., Pillitteri, V., 2024, Special publication 800-171, protecting controlled unclassified information in nonfederal systems and organizations, URL https://doi. org/10.6028/NIST.SP.800-171r3
- [ITTN-074], Silva, C., 2024, Pixel Zone Technology Control Plan, URL https://ittn-074.1sst. io/,

Vera C. Rubin Observatory ITTN-074

[ITTN-070], Silva, C., Hoblitt, J., 2023, Rubin Observability Project, URL https://ittn-070.lsst. io/,

Vera C. Rubin Observatory ITTN-070

[ITTN-045], Tapia, D., Silva, C., 2023, Summit Onboarding Procedure, URL https://ittn-045. lsst.io/,

Vera C. Rubin Observatory ITTN-045

[ITTN-010], Thebo, A., Hoblitt, J., 2023, User Identification and Authorization, URL https://
ittn-010.lsst.io/,
Vera C. Rubin Observatory ITTN-010

### C Acronyms

Acronym	Description
AAA	Authentication, Authorization and Accounting
AC	Access Control
AES	Advanced Encryption Standard
AT	Awareness and Training
AU	Audit and Accountability
AURA	Association of Universities for Research in Astronomy
CA	Certification, Accreditation, and Security Assessments
ССВ	Change Control Board
СМ	Configuration Management
СР	Contingency Planning



CUI	Controlled Unclassified Information
DM	Data Management
DMTN	DM Technical Note
DWDM	Dense Wave Division Multiplex
EOL	End of Life
IA	Identification and Authentication
IPA	FreeIPA - Identity, Policy, Audit
IR	Incident Response
ISO	Information Security Officer
IT	Information Technology
ITTN	IT Technote
LHN	long haul network
MA	Maintenance
MAC	Media Access Control
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology (USA)
NOIRLab	NSF's National Optical-Infrared Astronomy Research Laboratory; https://
	noirlab.edu
NSF	National Science Foundation
OPS	Operations
015	operations
013 05	Operating System
OS	Operating System
OS PE	Operating System Physical and Environmental Protection
OS PE PL	Operating System Physical and Environmental Protection Planning
OS PE PL PS	Operating System Physical and Environmental Protection Planning Personnel Security
OS PE PL PS PZ	Operating System Physical and Environmental Protection Planning Personnel Security photo-z
OS PE PL PS PZ RA	Operating SystemPhysical and Environmental ProtectionPlanningPersonnel Securityphoto-zRisk Assessment
OS PE PL PS PZ RA RTN	Operating SystemPhysical and Environmental ProtectionPlanningPersonnel Securityphoto-zRisk AssessmentRubin Technical Note
OS PE PL PS PZ RA RTN S3	Operating SystemPhysical and Environmental ProtectionPlanningPersonnel Securityphoto-zRisk AssessmentRubin Technical Note(Amazon) Simple Storage Service
OS PE PL PS PZ RA RTN S3 SA	Operating SystemPhysical and Environmental ProtectionPlanningPersonnel Securityphoto-zRisk AssessmentRubin Technical Note(Amazon) Simple Storage ServiceSystem and Services Acquisition
OS PE PL PS PZ RA RTN S3 SA SC	Operating SystemPhysical and Environmental ProtectionPlanningPersonnel Securityphoto-zRisk AssessmentRubin Technical Note(Amazon) Simple Storage ServiceSystem and Services AcquisitionSystem and Communications Protection
OS PE PL PS PZ RA RTN S3 SA SC SI	Operating SystemPhysical and Environmental ProtectionPlanningPersonnel Securityphoto-zRisk AssessmentRubin Technical Note(Amazon) Simple Storage ServiceSystem and Services AcquisitionSystem and Communications ProtectionSystem and Information Integrity



SQR	SQuARE document handle
SSID	Service Set Identifier
SSL	Secure Sockets Layer
USB	Universal Serial Bus
USDF	United States Data Facility
UTC	Coordinated Universal Time
VPN	virtual private network
VRO	(not to be used)Vera C. Rubin Observatory