

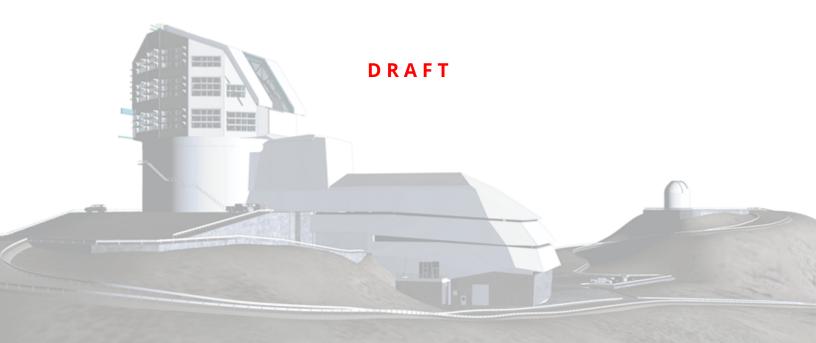
# Vera C. Rubin Observatory Data Management

# Rubin Observatory Data Security Standards Response

William O'Mullane, Russ Allbery, Yusra AlSayyad, Eric Bellm, Andy Clements, Richard Dubois, Joshua Hoblitt, Cristián Silva, Ian Sullivan, Kian-Tat Lim

**DMTN-199** 

Latest Revision: 2022-01-31





### **Abstract**

This is a response to the security document from the agencies.





# **Change Record**

| Version | Date       | Description                                  | Owner name        |
|---------|------------|--|-------------------|
| 0.1     | 2021-07-19 | Unreleased. Set up structure                 | William O'Mullane |
| 0.2     | 2021-09-28 | Unreleased. First draft for JSR 2021         | William O'Mullane |
| 0.3     | 2021-10-04 | Unreleased. Second draft for JSR 2021        | William O'Mullane |
| 0.4     | 2021-10-05 | Unreleased. Tidy for JSR 2021                | William O'Mullane |
| 0.5     | 2021-11-23 | Unreleased. Fix router price, inclide Huawei | William O'Mullane |
|         |            | Avoid  |                   |

Document source location: https://github.com/lsst-dm/dmtn-199

DRAFT iii DRAFT



#### **Contents**

| 1 | Introduction   | 1  |
|---|--|----|
| 2 | Cost Summary   | 2  |
| 3 | Response to the requirements   | 2  |
|   | 3.1 Encrypt Data   | 3  |
|   | 3.2 Install Firewalls and other physical security devices            | 4  |
|   | 3.3 Delay public release   | 6  |
|   | 3.4 Eliminate earth orbiting satellites                              | 8  |
|   | 3.5 Perform earth orbiting satellite processing in separate facility | 8  |
|   | 3.6 Publish nominal schedule   | 8  |
|   | 3.7 Request approval for non sidereal tracking                       | 9  |
| 4 | Conclusion   | 9  |
| Α | Compliance with NIST Standard  | 10 |
| В | References   | 14 |
| C | Acronyms   | 15 |



#### Rubin Observatory Data Security Standards Response

#### 1 Introduction

The agencies have provided a set of requirements for data security which are addressed in this upgrade plan. This document addresses the upgrades specifically and will augment the overall security plan for Rubin observatory (see LDM-324). This document addresses the specific requirements given to us by the agencies.

The summary of requirements are:

- 1. Encrypt data using strong, approved encryption standard, following NIST 800-171 standard for non-federal organizations.
- 2. Install firewalls to prevent unauthorized network access, guided by NIST 800-171 standard for non-federal organizations.
- 3. Delay public release of focal plane scientific data for at least 80 hours following the observation, with Alert Vetting System allowed to withhold up to 4 images per month for up to 10 days with need only for notification to be given to NSF/DOE. Delay public release of engineering and commissioning imaging data for at least 30 days.
- 4. Eliminate artificial Earth-orbiting satellites from prompt alerts by (a) automatically alerting only on streaks corresponding to motions slower than 30 deg/day relative to sidereal tracking, and (b) alerting on longer (faster) streaks only after the Alert Vetting System has determined that the streak does not correspond to an artificial satellite.
- 5. Perform Earth-orbiting satellite processing in a separate facility operated by a "trusted broker" that has access to appropriate satellite catalogs.
- 6. Publish nominal collection schedules for regular sky survey 24 hours in advance.
- 7. Request and receive advance approval of large sky regions for use without sidereal tracking prior to initial on-sky test observations; then, approved regions (for use without sidereal tracking) will be supplied to the Rubin Observatory operations team in advance of their use.

Section 3 provides a subsection response for each of these bullets.

DRAFT 1 DRAFT



#### **2 Cost Summary**

A summary of the costs associated with implementing these enhanced security measures are summarized in Table 1 below. The table includes both non-recurring, up-front, costs as well as the costs to operated with these enhanced measures for a 10-year operation period. Table 1 gives a summary.

Table 1: This table provides an overview of all the costs associated with this change.

| Item                                      | Cost        | <b>Operations Cost</b> |
|---|-------------|------------------------|
| Encryption (Table 2)                      | \$5,242,250 | \$3,441,000            |
| Firewalls and physical security (Table 3) | \$1,428,624 | \$4,800,000            |
| Delayed Data Store (Table 4)              | \$800,000   | \$800,000              |
| Alert Vetting System (Table 5) ROP value  |             | \$13,662,042           |
| Total Construction                        | \$7,470,874 |                        |
| Total Operations Cost                     |             | \$22,703,042           |

Execution of this plan will begin immediately upon approval to complete the changes prior to data collection in the system commissioning phase of Construction.

#### 3 Response to the requirements

This plan follows the applicable elements of NIST.SP.800-171. The application of this standard to the Rubin Observatory requires some interpretation. A compliance matrix is provided in Appendix A. In this matrix and in this document we assume the requirements apply to embargoed images before release to the collaboration and the derived difference image sources. Hence it applies to Prompt Processing, the embargoed data store(s), and the summit in Chile. It does not apply to DACs nor the actual alert stream.

The non-recurring costs in this plan include necessary end-equipment to manage the data entering the USDF. The incrimental operating costs at the USDF, expecting that they too will follow NIST 800-171, are provided in this document as reference.

DRAFT 2 DRAFT



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

#### 3.1 Encrypt Data

As outlined in DMTN-108 we shall buy four routers which can perform IPsec AES-256 bit encryption between Chile and SLAC. We will not transfer embargoed images to France - hence we should keep a secure data store at Chile and at SLAC for redundancy. The router cost in Table 2 is based on a quotation from Cisco as one of the vendors explicitly specified in the agency document. While we have shown that TLS with AES-256 can provide sufficient performance to meet our Alert timing budget, we have not yet measured performance with the specified routers using IPsec. We assume that performance will be adequate.

NIST also suggests out of band access - an independent network for access to the Summit systems in case the main network is down. A quote for Telconor to give a backup control link is included in Table 2.

See Table 2 for the cost breakdown. The OOB access is in Chile only and the routers and cabling are an even split.

Table 2: This table provides cost estimates for encrypted data transfer.

| Item                                     | Cost        | number | Total       |
|--|-------------|--------|-------------|
| Cisco Router (2@Chile 2@SLAC)            | \$500,000   | 4      | \$2,000,000 |
| Cabling                                  | \$1,000     | 4      | \$4,000     |
| Out of Bounds (OOB) link install (Chile) | \$60,000    | 2      | \$120,000   |
| HuaWei Aviod IRU                         | \$2,390,000 | 1      | \$2,390,000 |
| HuaWei Aviod installation                | \$600,000   | 1      | \$600,000   |
| HuaWei Aviod equipment                   | \$117,000   | 1      | \$117,000   |
| HuaWei Avoid FIU overhead                | \$11,250    | 1      | \$11,250    |
| Total Construction                       |             |        | \$5,242,250 |
| OOB Ops running cost/month               | \$3,000     | 240    | \$720,000   |
| Router rehresh                           |             |        | \$2,000,000 |
| Cabling                                  | \$1,000     | 4      | \$4,000     |
| HuaWei Aviod Maint 3%x10 years           | \$71,700    | 10     | \$717,000   |
| Total Operations                         |             |        | \$3,441,000 |

<sup>&</sup>lt;sup>1</sup>{confidentiality, availability, integrity}

DRAFT 3 DRAFT



#### 3.2 Install Firewalls and other physical security devices

This requirement is for physical and cyber security. It includes installing cameras and locks on racks. Some of this such as Firewalls is already in the project plan but much of it is not.

Items already in the baseline include:

- Card access to server rooms.
- Backup network in case main link fails (though the microwave link is a new addition ..)
- Auditable process to handle onboarding/offboarding
- Some cameras are in the project but not complete coverage.

The firewalls and physical security will be upgraded to meet the enhanced standard. Table 3 includes the items needed for this upgrade.

**Important Note**: We shall ring fence the Camera in its own firewall with more restricted access than the restricted control network. However we will treat it as a black box deliverable for this requirement. We shall not expect encryption of the internal disks of the camera system. Any perturbation to the camera system will have a deleterious effect on the camera with significant development and schedule impacts.

Signage and labeling, as required in NIST 171 3.8.4 <sup>2</sup>, will be developed as appropriate.

NIST 1.7.1 Section 3.10.6 pulls in extra standards for remote work namely NIST.800-46 and NIST.800-114. NIST.800-114 is the broader scope and we are pretty much in line with how it is written - we note Section 5.2.1 that we use Onepassword as a vault for IT passwords - not paper in a fire proof safe as recommended. Some other suggestions are understood to be useful in general but often not suitable for developers - personal firewalls, application filtering and aggressive antivirus software often trip over developer code and tools.

NIST.800-46 and other related NIST documentation suggest threat modeling - we do this in a limited way e.g SQR-041 and SQR-037. A more exhaustive risk assessment by a third party is

DRAFT 4 DRAFT

<sup>&</sup>lt;sup>2</sup>https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf



not anticipate at this time but the PRoject team will discuss with SLAC on any plans to review the USDF. We do not store sensitive information on the VPN nor bastion nodes. We do use NAT in a limited number of places - this will be more important in operations if/when we move to IPv6.

Table 3: This table provides cost estimates for firewalls and other physical security in Chile and at SLAC not in the project plan.

| Item  | Cost     | number | Total       |
|---|----------|--------|-------------|
| Locks SLAC                                      | \$200    | 30     | \$6,000     |
| Cameras Detectors SLAC                          | \$2,000  | 1      | \$2,000     |
| Sensors SLAC                                    | \$38     | 30     | \$1,140     |
| Sensor hub SLAC                                 | \$448    | 1      | \$448       |
| Locks Chile                                     | \$200    | 30     | \$6,000     |
| Cameras Detectors Chile                         | \$2,000  | 2      | \$4,000     |
| Sensors Chile                                   | \$38     | 30     | \$1,140     |
| Sensor hub Chile                                | \$448    | 2      | \$896       |
| Faster CPU to handle disk encryption on summit  | \$13,000 | 20     | \$260,000   |
| (node price)                                    |          |        |             |
| SSD price differnce to SATA (cost/TB)           | \$250    | 260    | \$65,000    |
| Labor to redeploy all summit systems (contract) | \$100    | 1,200  | \$120,000   |
| Labelling and signage                           | \$2,000  | 1      | \$2,000     |
| Security related contracts/month                | \$40,000 | 24     | \$960,000   |
| Operations Security contracts                   | \$40,000 | 120    | \$4,800,000 |
| Total Construction                              |          |        | \$1,428,624 |
| Total Operations                                |          |        | \$4,800,000 |

This enhance security plan includes support from an outside security provider. It is estimated running an SOC could cost upward of \$1.4M per year<sup>3</sup>. This article<sup>4</sup> outlines the pros and cons of an outsourced SOC and estimates it at between 300 and 800K per year. For budgetting purposes \$40K a month is included in Table 3. Such a contract (or contracts) should cover:

- 1. Proactive monitoring and alerting (NIST 171 section 3.3.5)
  - Write alerts for suspicious behaviors
  - Analyze collected logs for anomalies
- 2. Root cause analysis of any alert or anomaly
- 3. Incident response
  - Isolation of attacker
  - Forensic analysis leading to timeline and inventory of compromise
  - · Identifying systems that will need to be rebuilt

DRAFT 5 DRAFT

<sup>&</sup>lt;sup>3</sup>https://expel.io/blog/how-much-does-it-cost-to-build-a-24x7-soc/

 $<sup>^4</sup> https://www.linkbynet.com/outsourced-soc-vs-internal-soc-how-to-choose$ 



- 4. Vulnerability scanning including filtering out false positives
- 5. Asset inventory including patch status
- 6. Penetration testing to proactively look for vulnerabilities

This will require extensive coordination and integration with existing IT services and processes, included as part of this cost.

Since we will have to encrypt systems on the summit (see ITTN-014) for a list of systems) we anticipate upgrade processors and solid state drives (SSD) are required. Determining the detailed specifications will require experimentation so the values in the table for this are engineering estimates.

Note that compute facilities for the Commissioning Cluster at the Base as well as Alert Production and the Staff RSP at the USDF are not considered to be within the physical security area. Rubin considers the short-term, ephemeral processing on these resources outside of the enhanced security requirmenets. Including them would approximately double the cost of this item for Construction.

#### 3.3 Delay public release

Rubin considers the best approach to managing public release of data is to keep the embargoed data on a secure device separate from other systems and migrate images to the regular repository as they become *public*. This can be an object store with encryption like MinIO  $^5$ . We will need to have one at SLAC and one at Chile for redundancy to ensure no data loss.

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

The nominal embargo for regular operations we understand as between 80 hours (most images) and 10 days (some images as specified by Alert Vetting).

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

DRAFT 6 DRAFT

<sup>&</sup>lt;sup>5</sup>https://min.io/product/enterprise-object-storage-encryption



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

**Note:** Te enact these enhanced security measures on Commissioning data, this plan focuses on early data processeing at the SLAC USDF and not the resources originally planned at NCSA. The SLAC USDF must be ready h sufficient services and capcity for ComCam, on sky work.

Figure 1 depicts the encrypted storage and network. Embargoed (delayed) data would be held in the encrypted stores for the time specified. We assume temporary processing for alerts does not have to be encrypted, NIST allows ephemeral unencrypted data for processing.

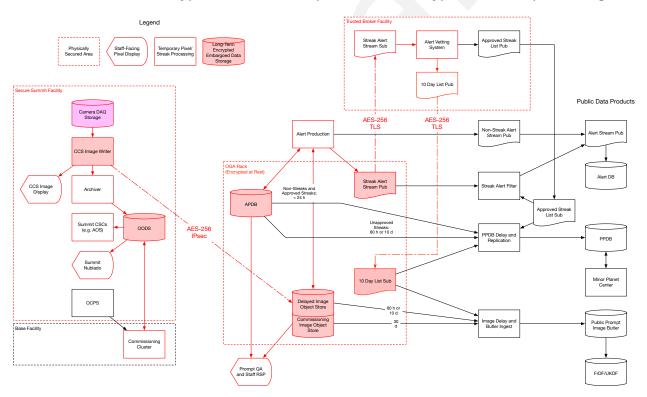


FIGURE 1: OGA architecture showing the long term encrypted storage and encrypted network from Chile to SLAC.

DRAFT 7 DRAFT



#### 3.4 Eliminate earth orbiting satellites

Rubin does not publish alerts for streaks associated with artificial satellites. A subset of streaks, potentially consistent with Earth-orbiting satellites or Solar System objects, will be evaluated by the AVS. AVS is under discussion currently in terms of design and how it may be implemented. The cost here is based on FTE and non labor after initial discussions with LLNL. They are assuming a high availability service. An estimate is given in Table 5. This also includes the current value in the operations plan. The cost of delaying the data in an encrypted store is already covered in Section 3.3

Cost Count Total Description FTE per year \$416,000 \$1,081,600 2.6 Mission years 10 \$10,816,000 \$1,000,000 \$2,000,000 Pre operations years 2 non labor 1 off \$611,000 1 \$611,000 non labor recurring \$25,000 \$250,000 Total \$13,677,000 Rubin Operations Plan Value \$13,662,042

Table 5: The Alert Vetting System is all FTE cost - apart from unknown hardware at LLNL.

#### 3.5 Perform earth orbiting satellite processing in separate facility

This is under discussion with LLNL - initial cost estimates are given in Section 3.4. It is shown in Figure 1.

#### 3.6 Publish nominal schedule

The project was already planning to publish the observing schedule to allow co observing of sources, see Section 2.1 of LSE-30. The OSS requires publication at least two hours ahead of observing - the request here is to have the schedule twenty four hours in advance. This is not a problem as long as one understands the fidelity of the schedule decreases with the look ahead time. The agency requirement acknowledges this.

The schedule is to be delivered to the trusted broker - we shall arrange this with LLNL.

We consider no delta cost for this as it was in the project plan.

DRAFT 8 DRAFT



#### 3.7 Request approval for non sidereal tracking

This is best handled Procedurally and as such will not produce a delta cost on the project.

#### 4 Conclusion

We can comply with the requirements and NIST 1.7.1 at the cost outlined in Section 2.

There are a few assumptions explicitly made above which we feel comply with given requirements but did require interpretation. To be explicit:

- Section 3 Assumes embargoed images before release to the collaboration are treated securely. After the embargo is lifted there is no longer a need to secure the images at the higher requirements.
- Section 3 Assumes NIST 1.7.1 also applies to SLAC even though NIST.FIPS.200 should be applicable.
- Section 3.2 Makes an important note about not encrypting internal camera storage.
- Section 3.2 Assumes NIST.800 documents were written as guidance they will be noted but we may not always follow all recommendations in all cases.
- Section 3.3 Assumes the 30 day embargo for commissioning applies to use of encrypted storage and transfers. This potentially implies NCSA could not be used for commissioning at all.
- Section 3.2 and Section 3.3 Assumes short stays of data on unencrypted machines for processing is ok (it is in line with NIST).

DRAFT 9 DRAFT



## **A** Compliance with NIST Standard

Table 6: This table provides an overview of the NIST.SP.800-171 and Rubin compliance with it.

| NIST 800-171  | 2021<br>Status | Intended<br>Compli-<br>ance | Note   |
|---|----------------|-----------------------------|--|
| 3.1 ACCESS CONTROL  |                |                             |  |
| 3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).   | Y              | Y                           |  |
| 3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.  | N              | Y                           | There are many non-administrative users with unrestricted sudo access, this will be addressed.   |
| 3.1.3 Control the flow of CUI in accordance with approved authorizations.   | Υ              | Y                           |  |
| 3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.   | N              | Y                           | Principle of least privilege is applied. Many users have access to hosts that is unneeded.   |
| 3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.   | N              | Y                           | Targeted sudo rules are needed for common operations. IPA controls sudo centrally  |
| 3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.  | Υ              | Y                           |  |
| 3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.   |                | Y                           | This is probably sudo attempts audits. Full commands can be logged in at the cost of extra load for the servers.   |
| 3.1.8 Limit unsuccessful login attempts.  | N              | Y                           | I don't believe we do this now but we can; this is not done for ssh on hosts or network equipment. Web Services such as love, foreman, ipa console, nublado, etc. may need rate limiting [Cristian: we dont use passwords in ssh hosts, it's only ssh keys so technically we are limiting the access to a single attempt.] |
| 3.1.9 Provide privacy and security notices consistent with applicable CUI rules.  | N              | Y                           | Check login notices etc. A login banner can be displayed upon login  |
| 3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.  | Y              | Y                           | This is our policy.  |
| 3.1.11 Terminate (automatically) a user session after a defined condition.  | N              | Y                           | ssh sessions are generally not limited on hosts; some network equip-<br>ment has timeouts set; nublado has a session limit for notebooks?  |
| 3.1.12 Monitor and control remote access sessions.  | N              | Y                           | We currently check who and from where is connecting.   |
| 3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.  | Y              | Y                           | VPN is in use  |
| 3.1.14 Route remote access via managed access control points.   | N              | Y                           | Bastion nodes – LHN is an open back door with no ACLs  |
| 3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.  | Y              | Y                           | ·  |
| 3.1.16 Authorize wireless access prior to allowing such connections.  | Υ              | Y                           | All devics attaching in Chile need to be registered by Mac address.  |
| 3.1.17 Protect wireless access using authentication and encryption.   | Υ              | Y                           |  |
| 3.1.18 Control connection of mobile devices.  | Υ              | Y                           | In the sense there is no open wifi, and on the summit devices must be registered.  |
| 3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23  | Y              | Y                           | Data will not exist on mobile devices - in the case where an image may exist on say commissioning team laptop we will have disk encryption enabled.  |
| 3.1.20 Verify and control/limit connections to and use of external systems.   | Y              | Y                           | This implies vetting of devices that connect to the control network - we use mac address for laptops and personal mobile phones can not connect to the control network. [Cristian: we already have a separation with the LHN SSID and VLANS]   |
| 3.1.21 Limit use of portable storage devices on external systems.   | N              | Y                           | Can be rolled out with puppet but there are some servers that need usb.  |
| 3.1.22 Control CUI posted or processed on publicly accessible systems. 3.2 AWARENESS AND TRAINING   | Υ              | Y                           | We do not intend to post images on publicly accessible systems.  |
| 3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. | Y              | Y                           |  |
| 3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.   | N              | Y                           |  |
| 3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.  | Y              | Y                           | We would like to do more here like capture flag exercises for developers or blue/red teams events  |
| 3.3 AUDIT AND ACCOUNTABILITY  |                |                             |  |
| 3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.  | Y              | Y                           |  |
| 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.  | Y              | Y                           |  |
| 3.3.3 Review and update logged events.  | Р              | Υ                           | We may look for a third party contract for this.   |
| 3.3.4 Alert in the event of an audit logging process failure.   | N              | Υ                           |  |

DRAFT 10 DRAFT



| 3.3.5 Correlate audit record review, analysis, and reporting processes for investigation   | N | Υ        | Again shall look for third party contract for this  |
|--|---|----------|---|
| and response to indications of unlawful, unauthorized, suspicious, or unusual activity.  |   |          |   |
| 3.3.6 Provide audit record reduction and report generation to support on-demand  | N | Y        |   |
| analysis and reporting.  |   |          |   |
| 3.3.7 Provide a system capability that compares and synchronizes internal system   | Y | Y        |   |
| clocks with an authoritative source to generate timestamps for audit records.  3.3.8 Protect audit information and audit logging tools from unauthorized access, | Y | Y        |   |
| modification, and deletion.  | Y | Y        |   |
| 3.3.9 Limit management of audit logging functionality to a subset of privileged users.   | Y | Y        |   |
| 3.4 CONFIGURATION MANAGEMENT   | ' | +        |   |
| 3.4.1 Establish and maintain baseline configurations and inventories of organizational   | Y | Y        | We use mainly infrastructure as code approaches so the software is  |
| systems (including hardware, software, firmware, and documentation) throughout   | ' | '        | we use mainly min astructure as code approaches so the software is well tracked. IT inventory all the hardware. |
| the respective system development life cycles.   |   |          | went tracked. It inventory all the hardware.  |
| 3.4.2 Establish and enforce security configuration settings for information technology   | Υ | Y        |   |
| products employed in organizational systems.   |   | '        |   |
| 3.4.3 Track, review, approve or disapprove, and log changes to organizational sys-   | Υ | Υ        | We have CCBs and code change process in place which also cover  |
| tems.  | - |          | the infrastructure as code.   |
| 3.4.4 Analyze the security impact of changes prior to implementation.  | Υ | Y        |   |
| 3.4.5 Define, document, approve, and enforce physical and logical access restrictions  | Υ | Y        |   |
| associated with changes to organizational systems.   |   |          |   |
| 3.4.6 Employ the principle of least functionality by configuring organizational systems  | N | Υ        |   |
| to provide only essential capabilities.  |   |          |   |
| 3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports,  | Υ | Υ        | We get a lot of this by mainly containerizing the applications and  |
| protocols, and services.   |   |          | having users work within deployed containers.   |
| 3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized   | N | Υ        | We need to implement SUDO lists to restrict access. However, this   |
| software or deny-all, permit-by-exception (whitelisting) policy to allow the execution   |   |          | could be related to blacklisting of applications.   |
| of authorized software.  |   |          |   |
| 3.4.9 Control and monitor user-installed software.   | Υ | Υ        |   |
| 3.5 IDENTIFICATION AND AUTHENTICATION  |   |          |   |
| 3.5.1 Identify system users, processes acting on behalf of users, and devices.   | Υ | Υ        |   |
| 3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a pre-   | Υ | Υ        |   |
| requisite to allowing access to organizational systems.  |   |          |   |
| 3.5.3 Use multifactor authentication for local and network access to privileged ac-  | N | Υ        | Chile dont require 2FA at the moment  |
| counts and for network access to non-privileged accounts.  |   |          |   |
| 3.5.4 Employ replay-resistant authentication mechanisms for network access to priv-  |   | Y        | Chile dont require 2FA at the moment, but certificates are deployed   |
| ileged and non- privileged accounts.   |   | <u> </u> | to prevent mitm   |
| 3.5.5 Prevent reuse of identifiers for a defined period.   | N | Y        |   |
| 3.5.6 Disable identifiers after a defined period of inactivity.  | Y | Y        |   |
| 3.5.7 Enforce a minimum password complexity and change of characters when new  | Y | Y        |   |
| passwords are created.  3.5.8 Prohibit password reuse for a specified number of generations.   | Y | Y        |   |
| 3.5.9 Allow temporary password use for system logons with an immediate change to   | Y | Y        |   |
| a permanent password.  | 1 | '        |   |
| 3.5.10 Store and transmit only cryptographically-protected passwords.  | Υ | Y        |   |
| 3.5.11 Obscure feedback of authentication information.   | Y | Y        |   |
| 3.6 INCIDENT RESPONSE  |   | <u>'</u> |   |
| 3.6.1 Establish an operational incident-handling capability for organizational systems   | Y | Y        | AURA have insurance which covers this. But we really should have a  |
| that includes preparation, detection, analysis, containment, recovery, and user re-  |   | '        | contract to look over logs etc. to note when we are hit.  |
| sponse activities.   |   |          |   |
| 3.6.2 Track, document, and report incidents to designated officials and/or authorities   | Υ | Υ        |   |
| both internal and external to the organization.  |   |          |   |
| 3.6.3 Test the organizational incident response capability.  | N | Υ        |   |
| 3.7 MAINTENANCE  |   |          |   |
| 3.7.1 Perform maintenance on organizational systems.   | Υ | Υ        |   |
| 3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to   | Υ | Υ        |   |
| conduct system maintenance.  |   |          |   |
| 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.   | Υ | Υ        |   |
| 3.7.4 Check media containing diagnostic and test programs for malicious code before  | Υ | Υ        |   |
| the media are used in organizational systems.  |   |          |   |
| 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions  | N | Υ        | Chile dont do 2FA yet. DUO has the capability to kill sessions.   |
| via external network connections and terminate such connections when nonlocal  |   |          |   |
| maintenance is complete.   |   |          |   |
| 3.7.6 Supervise the maintenance activities of maintenance personnel without re-  | Υ | Υ        |   |
| quired access authorization.   |   |          |   |
| - 1  |   |          |   |
| 3.8 MEDIA PROTECTION   |   |          |   |
| 3.8 MEDIA PROTECTION     3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.                        | N | Y        |   |

DRAFT 11 DRAFT



| 8.8.3 Similar of ectory optem media to authorized disposal or release for Y V Y  8.8.4 Similar or develop optem media containing CUI and disposal or release for Y V Y  8.8.5 Control across to media containing CUI and maintain accountability for media during transport cutosité of corrolled areas.  8.8.5 Control across to media containing CUI and maintain accountability for media during transport cutosité of corrolled areas.  8.8.5 Control across to media containing CUI and maintain accountability for media during transport unless whereives protected by alternative and disposal media during transport unless whereives protected by alternative and disposal media during transport unless whereives protected by alternative and disposal media during transport unless whereives protected by alternative and disposal media during transport unless whereives protected by alternative and disposal media during transport unless whereives protected by alternative and disposal media during transport unless whereives protected by alternative and disposal media during transport unless whereives protected by alternative and disposal media during transport unless whereives protected by a disposal media during transport unless and protected during and alternative and transport and transport transpor                                  |  |                   |                   |   |
|---|--|-------------------|-------------------|---|
| 1.8.3 Sancter or destroy system media containing CUI before disposal or release for vivor.  3.8.4 Mark media with necessary CUI markings and distribution limitations.  3.8.5 Control access to media containing CUI and maintain accountability for media during transport unitsel destroy to the provision of the physical single interleanments to protect the confidentiality of CUI accessed by alternative physical single during transport unitsel software protected by alternative physical single during transport unitsel software protected by alternative physical single protect the confidentiality of backgo in the physical single protected by alternative physical single protected to protect the confidentiality of backgo. CUI at storage locations.  3.8.6 Forest the confidentiality of backgo CUI at storage locations.  3.9.7 Forest chief our with purport but there are some severs that need alto be control.  3.9.8 Forest this confidentiality of backgo CUI at storage locations.  3.9.9 FORESTANES, SECURITY  3.9.1 Security of backgo CUI at storage locations.  3.9.2 Forest that confidentiality of backgo CUI at storage locations.  3.9.2 Forest that confidentiality of backgo CUI at storage locations.  3.9.2 Forest that confidentiality of backgo CUI at storage locations.  3.9.2 Forest that confidentiality of backgo CUI at storage locations.  3.9.2 Forest that confidentiality of backgo CUI at storage locations.  3.9.2 Forest that confidentiality of backgo CUI at storage locations.  3.9.2 Forest that confidentiality of backgo CUI at storage locations.  3.9.2 Forest that confidential pytems containing CUI are protected during and after protected during                                   | 3.8.2 Limit access to CUI on system media to authorized users.   | N                 | Y                 |   |
| Als A Mark media with necessary CUI markings and distribution limitations.  8 As Control across to made contaming CUI and ministan accountability for media during transport sacistic of controlled areas.  8 As Control across to made contaming CUI and ministan accountability for media during transport sacistic enformations to protect the confidenciality of CUI asserted on digital media during transport unless otherwise protected by alternative physical safeguare.  8 As implement on protecting transport unless otherwise protected by alternative physical safeguare.  8 As implement on the origination of system components.  8 As in Problet to use of rentrolled across on system components.  9 As in Problet to use of protable storage devices when such devices have no identification of the confidenciality of baseling controlled across to origination of system containing CUI are protected during and after personnel activities and a controlled across to a semination and partners containing CUI are protected during and after personnel activities and a semination and interest containing CUI are protected during and after personnel activities and a semination and interest containing CUI are protected during and after personnel activities and a semination and interest containing CUI are protected during and after personnel activities and a semination and interest containing CUI are protected during and after personnel activities and a semination and interest containing CUI are protected during and after personnel activities and a semination and interest containing CUI are protected during and after personnel activities and a semination and areas and a markets.  1 as 10 As the control of the protect of the approach in section of the personnel activity and activities and activi                                  |  | V                 | V                 |   |
| 3.8.5 Control access to media contaming CUI and maintain accountability for media during transport outside of controlled areas.  3.8.5 Control access to media contaming CUI and maintain accountability for media during transport outside of controlled areas.  3.8.5 Control and maintain accountability of CUI and the use of portable storage devices when such devices have no identify that outside outside of portability of the cuit of portability of CUI as storage devices when such devices have no identify that outside the use of portability of the cuit of portabil                                  |  | '                 | '                 |   |
| ing to https://www.arches.gov/files/cui/20161256-cui-marking-bandbook v1.1.pdf  3.8.5 Control access to media containing CUI and manifelia accountability for media  3.8.6 Implement cyptographic mechanisms to protect the confidentiality of CUI  N  Y  Can be milled out with pupper but there are some servers that need up.  3.8.7 Control access to media containing CUI and protect the confidentiality of CUI  3.8.8 Probibit the use of removable media on systems components.  3.8.9 Protect the confidentiality of backup CUI at storage locations.  3.8.9 Protect the confidentiality of backup CUI at storage locations.  3.8.9 Protect the confidentiality of backup CUI at storage locations.  3.9 PRESCAMES EXCURITY  3.0.1 Screen influentiality of backup CUI at storage locations.  3.9 PRESCAMES EXCURITY  3.0.1 Screen influentiality of backup CUI at storage locations.  3.0.2 Ensure that organizational systems containing CUI are protected during and after personal actions such as attentions and transfers.  3.0.1 PRESCAMES EXCURITY  3.0.1 Screen influentiality of the control of the summart control of the control of the control of the summart control of the control of the control of the control of the control of th                                  | reuse.   |                   |                   |   |
| ing to https://www.arches.gov/files/cui/20161256-cui-marking-bandbook v1.1.pdf  3.8.5 Control access to media containing CUI and manifelia accountability for media  3.8.6 Implement cyptographic mechanisms to protect the confidentiality of CUI  N  Y  Can be milled out with pupper but there are some servers that need up.  3.8.7 Control access to media containing CUI and protect the confidentiality of CUI  3.8.8 Probibit the use of removable media on systems components.  3.8.9 Protect the confidentiality of backup CUI at storage locations.  3.8.9 Protect the confidentiality of backup CUI at storage locations.  3.8.9 Protect the confidentiality of backup CUI at storage locations.  3.9 PRESCAMES EXCURITY  3.0.1 Screen influentiality of backup CUI at storage locations.  3.9 PRESCAMES EXCURITY  3.0.1 Screen influentiality of backup CUI at storage locations.  3.0.2 Ensure that organizational systems containing CUI are protected during and after personal actions such as attentions and transfers.  3.0.1 PRESCAMES EXCURITY  3.0.1 Screen influentiality of the control of the summart control of the control of the control of the summart control of the control of the control of the control of the control of th                                  | 3.8.4 Mark media with necessary CLII markings and distribution limitations   | N                 | V                 | We understand we should label rooms and machines acord-   |
| AB.S. Control access to media containing CUI and maintain accountability for media during gramport outside of controlled areas.  3.8.F. Implement cytospophine medianous protects the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical Safetyper (cytospophine medianous protectes by alternative physical Safetyper (cytospophine medianous) protectes are some services that need to be a protected during and affect per promonel active subject protectes and the protected physical access and protected physical protectes and protected during and affect per protected during and affe                                  | 5.6.4 Walk media with necessary conmarkings and distribution innitiations.   | 11                | '                 |   |
| 1.8.5 Control access to media containing CUI and maintain accountability for media during transport under during transport under during transport under during transport under software under software under software under software under software un                                  |  |                   |                   | ing to https://www.archives.gov/files/cui/20161206-cui-marking-   |
| 1.8.5 Control access to media containing CUI and maintain accountability for media during transport under during transport under during transport under during transport under software under software under software under software under software un                                  |  |                   |                   | handbook-v1-1 ndf   |
| July grouper custode of controlled areas.  3.8.8 Implament cytopographic methanisms to protect the confidentiality of CUI storted on digital media during transport unless otherwise protected by alternative physical singuages.  3.8.7 Control the use of removable media on system components.  3.8.8 Profilest the confidentiality of backup CUI at storage bootions.  3.9 PRESCHANG SECURITY  3.9 PRESCHANG SECURITY  3.9 SECURITY  3.9 SECURITY  3.1 Screen involvables prior to authorizing access to organizational systems containing CUI.  3.9 SECURITY  4. Only project team members will have access to early images - all are introduction. The province of the profilest the confidentiality of backup CUI at storage bootions.  4. V  5.1 SECURITY  5.2 SECURITY  5.3 SECURITY  7. V  7. Only project team members will have access to early images - all are involved involved the access to early images - all are involved involved the access to early images - all are involved involved the access to early images - all are involved involved the access to early images - all are involved involved the access to early images - all are involved involved the access to early images - all are involved involved the access to early images - all are involved involved the access to early images - all are involved involved the access to early images - all are involved involved the access to early images - all are involved involved the access to early images - all are involved involved involved the access to early images - all are involved involved in the access to early images - all are involved involved in the access to early images - all are involved in the access to early images - all are involved in the access to early images - all are involved in the access to early images - all are involved in the access to early images - all are involved in the access to early images - all are involved in the a                                  |  |                   |                   | Harlabook VI 1.pai  |
| 1.38.6 implement cyptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical saregularities. In the confidentiality of backup CUI at storage locations.  2.3.8 Prohibit the use of portable storage devices when such devices have no identify that committee the confidentiality of backup CUI at storage locations.  2.3.8 Prohibit the use of portable storage devices when such devices have no identify that committee the confidentiality of backup CUI at storage locations.  2.3.1 SpressonMark SCLIGHTY  2.3.                                  | 3.8.5 Control access to media containing CUI and maintain accountability for media   | Y                 | Y                 |   |
| 1.38.6 implement cyptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical saregularities. In the confidentiality of backup CUI at storage locations.  2.3.8 Prohibit the use of portable storage devices when such devices have no identify that committee the confidentiality of backup CUI at storage locations.  2.3.8 Prohibit the use of portable storage devices when such devices have no identify that committee the confidentiality of backup CUI at storage locations.  2.3.1 SpressonMark SCLIGHTY  2.3.                                  | during transport outside of controlled areas   |                   |                   |   |
| Stored on digital media during transport unless otherwise protected by alternative physical storegues designed.  3.8.F rothist the use of portable storage devices when such devices have no identify that the use of portable storage devices when such devices have no identify that the use of portable storage devices when such devices have no identify that the use of portable storage devices when such devices have no identify that the use of portable storage devices when such devices have no identify that the use of portable storage devices when such devices have no identify that the use of portable storage devices when such devices have no identify that the use of portable storage devices when such devices have no identify that the use of portable storage devices when such devices have no identify that the use of portable storage devices when such devices have no identify that the use of portable storage devices when such devices have no identify that the use of portable storage devices when such devices have no identify that the use of portable storage devices when such devices have no identify that the use of portable storage in section of the requirements of the universal storage in the use of the requirements deviced in the use of the requirements document.  3.6.9 Ensoure that organizational systems containing CLI are protected during and after the proposal access in interest to the universal devices of the requirements to authorize the terminations and transfers.  3.1.0 PERSONAL STORAGE of the proposal access to organizational systems, quipment, and the respective operating memorizes to organizational systems, quipment, and the respective operating memorizes to organizational systems and support infrastructure for organizational systems and monitor vision activity.  3.1.0 Enforce are departed in the summit - contractors are considered memorizes of physical access to organizational systems and applications are identified.  3.1.1 Enrodically assess the risk to organizational systems and applications are identif                                  | <u> </u>   |                   |                   |   |
| Implicate safeguands.   3.8.7 control the use of protrable storage devices when such devices have no identificate owner.   3.8.8 Prohibit the use of portable storage devices when such devices have no identificate owner.   3.9 PERSONNEL SECURITY   Y   Y   Y   Y   Y   Y   Y   Y   Y  | 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI   | N                 | Y                 |   |
| Implicate safeguands.   3.8.7 control the use of protrable storage devices when such devices have no identificate owner.   3.8.8 Prohibit the use of portable storage devices when such devices have no identificate owner.   3.9 PERSONNEL SECURITY   Y   Y   Y   Y   Y   Y   Y   Y   Y  | stored on digital modia during transport unless otherwise protected by alternative   |                   |                   |   |
| 3.8.8 Prohibit the use of portable storage devices when such devices have no identify hable conner.  3.8.9 Prohibit the use of portable storage devices when such devices have no identify hable conner.  3.8.9 Protect the confidentiality of backup CUI at storage locations.  3.9.1 Streem individuals prior to authorizing access to organizational systems containing CUI.  3.9.2 Ensure that organizational systems containing CUI are protected during and after protected and monitoristic protections are protected and monitoristic protections and monitoristic protections and monitoristic protections.  3.10 PAYISCAL PROTECTION  3.10.1 English and a protection and monitoristic protections are consistent and monitoristic protections.  3.10.2 Excort visitors and monitoristic activity.  3.10.3 Excort visitors and monitoristic activity.  3.10.4 Monitoristic protections are consistent and monitoristic protections are activity.  3.10.5 Enforce softgained in protection and applications are identified from the operation of organizational systems and applications are identified to protect                                  |  |                   |                   |   |
| 1.3.8 Prohibit the use of portable storage devices when such devices have no identify hable cowner.  3.8.9 Protect the confidentiality of backup CUI at storage locations.  Y Y Y S.  3.9 Forces individuals prior to authorizing access to organizational systems containing CUI.  3.9 Ensure that organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organization and transfers.  Y Y This physical access limitation will increase with locks on server cabinates with a containing cut organization will increase with locks on server cabinates with a containing environments to authorize the device organization and monther the physical access devices.  N Y Y This physical access limitation will increase with locks on server cabinates with a containing environments or an area organizational systems.  N Y Child associates the access of the environment organization                                  | physical safeguards.   |                   |                   |   |
| 1.3.8 Prohibit the use of portable storage devices when such devices have no identify hable cowner.  3.8.9 Protect the confidentiality of backup CUI at storage locations.  Y Y Y S.  3.9 Forces individuals prior to authorizing access to organizational systems containing CUI.  3.9 Ensure that organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organizational systems containing CUI are protected during and afficient organization and transfers.  Y Y This physical access limitation will increase with locks on server cabinates with a containing cut organization will increase with locks on server cabinates with a containing environments to authorize the device organization and monther the physical access devices.  N Y Y This physical access limitation will increase with locks on server cabinates with a containing environments or an area organizational systems.  N Y Child associates the access of the environment organization                                  | 2.8.7 Control the use of removable media on system components  |                   | V                 | Can be rolled out with purpost but there are some servers that need   |
| 13.6.9 Protect the use of portable storage devices when such devices have no identify able owner.  3.8.9 Protect the confidentiality of backup CUI at storage locations.  3.9.2 Protect the confidentiality of backup CUI at storage locations.  3.9.2 Protect the confidentiality of backup CUI at storage locations.  3.9.2 Ensure that organizational systems containing CUI are protected during and affire protected affire protecting protecting protecting protecting protecting systems and monitor visitor activity.  4. V. This physical access to an affire protected during and affire protecting prot                                  | 3.8.7 Control the use of Terriovable media on system components.   |                   | '                 | Carrie Folled out with pupper but there are some servers that need  |
| fishle owner.       3.8.9 Protect the confidentiality of backup CUI at storage locations.       Y       Y         3.9 FIRSONNEL SECURITY       2.3.1 Streen individuals prior to authorizing access to organizational systems containing CUI.       Y       Only project team members will have access to early images: all are known individuals. This idean's suggest background security screening and art was also suggest background security screening and art was also suggest background security screening and it was also suggest background security of the program in a suggest background security and the certain of the program in a suggest background security and the certain of the program in a suggest background security of  |  |                   |                   | usb.  |
| fishle owner.       3.8.9 Protect the confidentiality of backup CUI at storage locations.       Y       Y         3.9 FIRSONNEL SECURITY       2.3.1 Streen individuals prior to authorizing access to organizational systems containing CUI.       Y       Only project team members will have access to early images: all are known individuals. This idean's suggest background security screening and art was also suggest background security screening and art was also suggest background security screening and it was also suggest background security of the program in a suggest background security and the certain of the program in a suggest background security and the certain of the program in a suggest background security of  | 2.9.0 Dyahihit the use of portable stayon devices when such devices have no identi-  | V                 |                   |   |
| 3.3 PERSONNES SCURITY  3.3 I Screen individuals prior to authorizing access to organizational systems containing CUI  3.3 I Screen individuals prior to authorizing access to organizational systems containing CUI  3.3 I Screen individuals prior to authorizing access to organizational systems containing CUI  3.3 I Screen individuals prior to authorizing access to organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.  3.10 I IVINISCAL PROTECTION  3.10.1 I IVINIS POSIS access to organizational systems, equipment, and the respective operating environments to authorized individuals.  3.10.2 Protect and monitor the physical racidity and support infrastructure for organizational systems.  4. Y  4. This physical access limitations will increase with locks on server cabiness (cf. but key card access is already in place.  3.10.2 Protect and monitor the physical racidity and support infrastructure for organizational systems.  5. Security in place or Department of the mountain monitor visitors activity.  5. Security in place or Department of the mountain monitor visitors activity.  7. Y  7. Accoult visitors are escorted on the summit contractors are considered monitor activity.  8. Accountain support infrastructure for organizational systems, and the association of the summit contractors are considered monitor with the summit contractors are considered monitor with the summit contractors are considered monitor and manage physical access devices.  9. Y  9. Y  9. Account visitors are secorted on the summit contractors are considered monitor and the summit contractors are considered monitors.  1.3.10.5 Control and manage physical access devices.  9. Y  1.3.11.1 Periodically assesses the risk to organizational systems and papications periodically undiversed to a contractive and papicational systems and papications are identified.  1.3.1.1.1 Periodically assesses the risk to organizational systems and applications periodically undiversed to organizational syste                                  | 3.8.8 Profibit the use of portable storage devices when such devices have no identi-   | T T               | l i               |   |
| 3.9 1 Streen individuals prior to authorizing access to organizational systems containing CUI.  3.9 1 Streen individuals prior to authorizing access to organizational systems containing CUI.  3.9 2 Ensure that organizational systems containing CUI are protected during and affirm the protection of the previous as terminations and transfers.  3.10 PHYSICAL PROTECTION  4. This physical access initiations will increase with locks on server cabinetic exception of the physical facility and support infrastructure for organizational systems.  3.10 PHYSICAL PROTECTION  4. This physical access initiations will increase with locks on server cabinetic exception of the physical phy                                  | fiable owner.  |                   |                   |   |
| 3.9 1 Streen individuals prior to authorizing access to organizational systems containing CUI.  3.9 1 Streen individuals prior to authorizing access to organizational systems containing CUI.  3.9 2 Ensure that organizational systems containing CUI are protected during and affirm the protection of the previous as terminations and transfers.  3.10 PHYSICAL PROTECTION  4. This physical access initiations will increase with locks on server cabinetic exception of the physical facility and support infrastructure for organizational systems.  3.10 PHYSICAL PROTECTION  4. This physical access initiations will increase with locks on server cabinetic exception of the physical phy                                  | 2.9.0 Divotost the confidentiality of hadron CIII at storage legations   | V                 | V                 |   |
| 33.15 Ercenindividuals prior to authorizing access to organizational systems containing CUI.  | 3.8.9 Protect the confidentiality of backup Col at storage locations.  | Ť                 | Y                 |   |
| 33.15 Ercenindividuals prior to authorizing access to organizational systems containing CUI.  | 3.9 PERSONNEL SECURITY   |                   |                   |   |
| Ing CUI.    Ing CUI.   In project of the project of                                  |  |                   | 1.4               |   |
| ing and it was also explicitly not required by the agencies in section 2 of the requirements document.  3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.  3.10 FMSIAL PROTECTION  3.10.1 Imit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.  3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.  3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.  3.10.3 Escont visitors and monitor visitor activity.  4. Y. Y. Actual visitors are exported on the summit - contractors are considered monitorial season.  5. Y. Y. Actual visitors are exported on the summit - contractors are considered more like seaff.  3.10.5 Enforce adapturating measures for CUI at alternate work sites.  4. Y. Y. This brings in NIST 800-46 and NIST,800-114. Threat analysis suggested. NAT considered bad.  3.1.1 RISK ASSESSMENT  3.1.1 Periodically assess the escentity control is norganizational systems and applications periodically and when new vulnerabilities in organizational systems and applications are identified.  3.1.2 Devote security controls on an anongoing basis to result in controls are effective in their application.  3.1.2 Provided lay assess the security controls in organizational systems to determine by the security controls on an anongoing basis to result of the controls.  3.1.2 Provided lay assess the security controls in organizational systems to determine by the security controls on an anongoing basis to result of the external boundaries and key internal boundaries of organizational systems to ensure the continues.  3.1.3.2 Monitor, control, and periodically update system security plans that described by organizational systems on a control to the extension security within organizational systems.  3.1.3.3.3 Ferrolic control, and periodically update system security plans tha                                  | 3.9.1 Screen individuals prior to authorizing access to organizational systems contain-  | Y                 | Y                 | Only project team members will have access to early images - all are  |
| ing and it was also explicitly not required by the agencies in section 2 of the requirements document.  3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.  3.10 FMSIAL PROTECTION  3.10.1 Imit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.  3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.  3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.  3.10.3 Escont visitors and monitor visitor activity.  4. Y. Y. Actual visitors are exported on the summit - contractors are considered monitorial season.  5. Y. Y. Actual visitors are exported on the summit - contractors are considered more like seaff.  3.10.5 Enforce adapturating measures for CUI at alternate work sites.  4. Y. Y. This brings in NIST 800-46 and NIST,800-114. Threat analysis suggested. NAT considered bad.  3.1.1 RISK ASSESSMENT  3.1.1 Periodically assess the escentity control is norganizational systems and applications periodically and when new vulnerabilities in organizational systems and applications are identified.  3.1.2 Devote security controls on an anongoing basis to result in controls are effective in their application.  3.1.2 Provided lay assess the security controls in organizational systems to determine by the security controls on an anongoing basis to result of the controls.  3.1.2 Provided lay assess the security controls in organizational systems to determine by the security controls on an anongoing basis to result of the external boundaries and key internal boundaries of organizational systems to ensure the continues.  3.1.3.2 Monitor, control, and periodically update system security plans that described by organizational systems on a control to the extension security within organizational systems.  3.1.3.3.3 Ferrolic control, and periodically update system security plans tha                                  | ing CUI.   |                   |                   | know individuals. This doesn't suggest background security screen-  |
| 3.3.2 Ensure that organizational systems containing CUI are protected during and affer personnel actions such as terminations and transfers.  3.10 PMSGAR POTECTION  3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.  3.10 PMSGAR POTECTION  3.10.1 Limit physical access to organizational systems, and upport infrastructure for organizational systems.  3.10 PMSGAR POTECTION  3.10.1 Limit physical access to organizational systems, and the respective operating environments to authorized individuals.  4. Y This physical access iminitations will increase with locks on server cabinets etc. but key card access is already in place.  5. Security is in place on Cero Pachon and at the entrance to the mountains that the properties of the control of the summit - contractors are considered more like staff.  5. A Chall wishfors are escorted on the summit - contractors are considered more like staff.  5. Chile use Notifical key-card system, we should reach to them to inquire about their audit procedures  3.10.5 Centrol and manage physical access devices.  7. Y This brings in NIST.800.46 and NIST.800-114. Threat analysis suggested. NAT considered bad.  3.11.1 Periodically assess the risk to organizational assets, and individuals, resulting from the operation of organizational systems and applications are identified.  3.11.2 Secondary organizational systems and applications are identified.  3.12.1 Periodically assess the security controls in organizational systems and applications are identified.  3.12.1 Periodically assess the security controls in organizational systems to determine of organizational systems and applications are identified.  3.12.1 Periodically assess the security controls in organizational systems.  3.12.2 Develop and implement plans of action designed to correct deficiencies and venture or all institute values of the controls.  3.13.2 Sincero and implement plans of action designed to correct deficiencies and venture or all insti                                  |  |                   |                   | 55 5  |
| 3.3.2 Ensure that organizational systems containing CUI are protected during and af-<br>tre personnel actions such as terminations and transfers. 3.10 PHYSICAL PROTECTION 3.10.1 Limit physical access to organizational systems, equipment, and the respective<br>operating environments to authorized individuals. 3.10.2 Protect and monitor the physical facility and support infrastructure for organi-<br>zational systems. 3.10.2 Protect and monitor the physical facility and support infrastructure for organi-<br>zational systems. 3.10.3 Escort visitors and monitor visitor activity.  3.10.3 Escort visitors and monitor visitor activity.  3.10.4 Maintain audit logs of physical access.  N Y Actual visitors are escorted on the summit - contractors are consid-<br>ered more like staff. 3.10.5 Control and manage physical access devices.  N Y Chile use Noriba key-card system, we should reach to them to in-<br>quiral about their audit procedures 3.11.1 Escort visitors are sufficiently assess the risk to organizational operations (including mission,<br>functions, image, or reputation), organizational assets, and individuals, resulting from<br>the operation of organizational systems and the associated processing, storage, or<br>transmission of CUI. 3.11.2 Escort Protect and monitor the physical access devices.  Y This brings in NIST.800-46 and NIST.800-114. Threat analysis sug-<br>gested. NAT considered bad.  Y Third party contract  Third party contract  Third party contract  Third party contract  And when new unlinerabilities in organizational systems and applications are identified.  3.11.2 Escort Protulenabilities affecting those systems and applications are identified.  3.12 Escort Protulenabilities in organizational systems and the associated processing, storage, or<br>transmission of CUI.  3.12 Develop and implement plans of action designed to correct deficiencies and evidence or eliminate vulnerabilities in organizational systems.  3.13 STEPTEM NID COMMUNICATIONS PROTECTION  3.13.1 Monitors control, and protect communications (i.e., information transferial |  |                   |                   | ing and it was also explicitly not required by the agencies in section  |
| 3.3.2 Ensure that organizational systems containing CUI are protected during and af-<br>tre personnel actions such as terminations and transfers. 3.10 PHYSICAL PROTECTION 3.10.1 Limit physical access to organizational systems, equipment, and the respective<br>operating environments to authorized individuals. 3.10.2 Protect and monitor the physical facility and support infrastructure for organi-<br>zational systems. 3.10.2 Protect and monitor the physical facility and support infrastructure for organi-<br>zational systems. 3.10.3 Escort visitors and monitor visitor activity.  3.10.3 Escort visitors and monitor visitor activity.  3.10.4 Maintain audit logs of physical access.  N Y Actual visitors are escorted on the summit - contractors are consid-<br>ered more like staff. 3.10.5 Control and manage physical access devices.  N Y Chile use Noriba key-card system, we should reach to them to in-<br>quiral about their audit procedures 3.11.1 Escort visitors are sufficiently assess the risk to organizational operations (including mission,<br>functions, image, or reputation), organizational assets, and individuals, resulting from<br>the operation of organizational systems and the associated processing, storage, or<br>transmission of CUI. 3.11.2 Escort Protect and monitor the physical access devices.  Y This brings in NIST.800-46 and NIST.800-114. Threat analysis sug-<br>gested. NAT considered bad.  Y Third party contract  Third party contract  Third party contract  Third party contract  And when new unlinerabilities in organizational systems and applications are identified.  3.11.2 Escort Protulenabilities affecting those systems and applications are identified.  3.12 Escort Protulenabilities in organizational systems and the associated processing, storage, or<br>transmission of CUI.  3.12 Develop and implement plans of action designed to correct deficiencies and evidence or eliminate vulnerabilities in organizational systems.  3.13 STEPTEM NID COMMUNICATIONS PROTECTION  3.13.1 Monitors control, and protect communications (i.e., information transferial |  |                   |                   | 2 of the requirements document  |
| ter personnel actions such as terminations and transfers.  3.10 PHYSICAL PROTECTION  3.10 Limit physical access to organizational systems, equipment, and the respective operating eminyer organizational systems, equipment, and the respective operating eminyer organizational systems.  3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.  3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.  3.10.3 Escort visitors and monitor visitor activity.  4 Y Security is in place on Cero Pachon and at the entrance to the mountain though not only for Rubin so not permanently at the observatory.  3.10.3 Escort visitors and monitor visitor activity.  5 Y Actual visitors are escorted on the summit - contractors are considered more like staff.  3.10.4 Maintain audit logs of physical access devices.  7 Y Chile use Noirfab key-card system, we should reach to them to inquire about the audit procedures.  3.10.5 Ecorter land manage physical access devices.  9 Y This physical access and systems with locks on server cables interested.  1.11 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assess, and individuals, resulting from the operation of organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications periodically and when new vulnerabilities affecting those systems and applications periodically and when new vulnerabilities in organizational systems to determine if the controls are reflective in their application.  1.12 ESCORITY ASSESSMENT  1.12 Periodically assess the security controls in organizational systems.  3.13 Escority Assessment and periodically systems and applications periodically and when new vulnerabilities in organizational systems.  3.13 Escority Assessment and periodically systems and applications periodically assess the security controls on an ongoing basis to ensure the continu                                  | 2005   | - V               | 1,,               | = 1 requirements accuments  |
| 3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. 3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems. 3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems. 3.10.3 Escort visitors and monitor visitor activity.  3.10.3 Escort visitors and monitor visitor activity.  3.10.4 Maintain audit logs of physical access.  N Y Actual visitors are escorted on the summit - contractors are considered more like staff. 3.10.5 Control and manage physical access devices.  3.10.5 Control and manage physical access devices.  3.11.6 Senforce safeguarding measures for CUI at alternate work sites.  Y Y This brings in NIST.800-46 and NIST.800-114. Threat analysis suggested. NAT considered bad.  3.11.1 Proficically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assess, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 SECURITY SSESSMENT  3.12.1 Periodically assess the security controls in organizational systems and the associated processing, storage, or transmission of CUI.  3.12.1 ESCURITY ASSESSMENT  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems and applications are identified.  3.13.2 ESCURITY controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.13.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.13.3 ESCURITY organizational systems and applications are elementative view of the controls or organizational systems.  3.13.3 ESCURITY organizational systems in companizational systems.  3.13.3 ESCURITY organizational properation organizational systems.  3.13.3 ESCURITY organizational systems in companizational sy                                  | 3.9.2 Ensure that organizational systems containing CUI are protected during and af-   | Y                 | Υ                 |   |
| 3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. 3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems. 3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems. 3.10.3 Escort visitors and monitor visitor activity.  3.10.3 Escort visitors and monitor visitor activity.  3.10.4 Maintain audit logs of physical access.  N Y Actual visitors are escorted on the summit - contractors are considered more like staff. 3.10.5 Control and manage physical access devices.  3.10.5 Control and manage physical access devices.  3.11.6 Senforce safeguarding measures for CUI at alternate work sites.  Y Y This brings in NIST.800-46 and NIST.800-114. Threat analysis suggested. NAT considered bad.  3.11.1 Proficically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assess, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 SECURITY SSESSMENT  3.12.1 Periodically assess the security controls in organizational systems and the associated processing, storage, or transmission of CUI.  3.12.1 ESCURITY ASSESSMENT  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems and applications are identified.  3.13.2 ESCURITY controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.13.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.13.3 ESCURITY organizational systems and applications are elementative view of the controls or organizational systems.  3.13.3 ESCURITY organizational systems in companizational systems.  3.13.3 ESCURITY organizational properation organizational systems.  3.13.3 ESCURITY organizational systems in companizational sy                                  | ter personnel actions such as terminations and transfers   |                   |                   |   |
| 3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. 3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems. 3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems. 3.10.3 Escort visitors and monitor visitor activity.  Y Security is in place on Cero Pachon and at the entrance to the mountain-though not only for Rubin so not permanently at the observatory. 3.10.3 Escort visitors and monitor visitor activity.  Y Actual visitors are escorted on the summit - contractors are considered under the staff. 3.10.4 Maintain audit logs of physical access.  N Y Chile use Noirfab keycard system, we should reach to them to inquire about and manage physical access devices. 3.10.5 Enforce safeguarding measures for CUI at alternate work sites.  Y Y This brings in NIST,800-46 and NIST,800-114. Threat analysis suggested. NAT considered bad. 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational aspitems and the associated processing, storage, or transmission of CUI. 3.11.2 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems and applications are identified. 3.12.2 SECURITY ASSESSMENT  3.12.2 Develop and implement plans of action designed to correct deficiencies and reflective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reflective information security controls in organizational systems. 3.13.3 Monitor security controls on an ongoing basis to ensure the continued effective endours are implemented, and the relationships with or connections to other systems. 3.13.3 SYELM ADD COMMUNICATION PROTECTION 3.13.3 SYELM ADD COMMUNICATION PROTE                                  | <u> </u>   |                   |                   |   |
| operating environments to authorized individuals. 3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems. 3.10.3 Escort visitors and monitor the physical facility and support infrastructure for organizational systems. 3.10.3 Escort visitors and monitor visitor activity.  V Y Actual visitors are escorted on the summit - contractors are considered more like staff. 3.10.4 Maintain audit logs of physical access.  N Y Y Chile woo horidab key-card system, we should reach to them to inquire about their audit procedures 3.10.5 Control and manage physical access devices. 3.10.5 Enforce safeguarding measures for CUI at alternate work sites.  V Y This brings in NIST 800-46 and NIST.800-114. Threat analysis suggested. NAT considered bad. 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and applications are identified. 3.12 Develop, document, and periodically update systems and applications are identified. 3.12.2 Develop, document, and periodically update systems security plans that describe system boundaries, system environments of operation how security requirements are implemented, and the relationships with or connections to other systems. 3.13.3 SYSTEM NA COMMINICATIONS PROTECTION 3.13.13 SYSTEM NA DOCOMMINICATIONS PROTECTION 3.13.13 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems and several boundaries and key internal boundaries of organizational systems) at the external boundaries and key internal boundaries of organizational systems in the external boundaries and key internal boundaries of organizational systems in the external boundaries and key internal boundaries of organizational systems) at the external boundaries and key internal boundaries of organizatio                                  | 3.10 PHYSICAL PROTECTION   |                   |                   |   |
| operating environments to authorized individuals. 3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems. 3.10.3 Escort visitors and monitor the physical facility and support infrastructure for organizational systems. 3.10.3 Escort visitors and monitor visitor activity.  V Y Actual visitors are escorted on the summit - contractors are considered more like staff. 3.10.4 Maintain audit logs of physical access.  N Y Y Chile woo horidab key-card system, we should reach to them to inquire about their audit procedures 3.10.5 Control and manage physical access devices. 3.10.5 Enforce safeguarding measures for CUI at alternate work sites.  V Y This brings in NIST 800-46 and NIST.800-114. Threat analysis suggested. NAT considered bad. 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and applications are identified. 3.12 Develop, document, and periodically update systems and applications are identified. 3.12.2 Develop, document, and periodically update systems security plans that describe system boundaries, system environments of operation how security requirements are implemented, and the relationships with or connections to other systems. 3.13.3 SYSTEM NA COMMINICATIONS PROTECTION 3.13.13 SYSTEM NA DOCOMMINICATIONS PROTECTION 3.13.13 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems and several boundaries and key internal boundaries of organizational systems) at the external boundaries and key internal boundaries of organizational systems in the external boundaries and key internal boundaries of organizational systems in the external boundaries and key internal boundaries of organizational systems) at the external boundaries and key internal boundaries of organizatio                                  | 2.10.1 Limit physical access to organizational systems, equipment, and the respective  | V                 | V                 | This physical access limitations will increase with locks on sonyer cab   |
| 3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.  3.10.3 Escort visitors and monitor visitor activity.  V Y Actual visitors are secored on the summit - contractors are considered more like staff.  3.10.4 Maintain audit logs of physical access.  N Y Chile use Noiriab key-card system, we should reach to them to inquire about their audit protecture.  3.10.5 Control and manage physical access devices.  3.10.5 Control and manage physical access devices.  3.10.6 Enforce safeguarding measures for CUI at alternate work sites.  3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems and applications are identified.  3.12.2 Eveloping and implement plans of action of assignment of controls are effective in their application.  3.12.2 Disciplination of compleximations of operation of paraizational plans of action of assignment of controls are effective in their application.  3.12.3 Interpretation of compleximation of controls in organizational systems of the controls are effective in their application.  3.12.2 Develop and implement plans of action of assignment the controls are effective in their application.  3.12.3 Eveloping and implement plans of action of assignment of controls are effective in their application.  3.13.4 SPCURITY or society in controls on an onaging basis to ensure the continued effectiveness of the controls.  3.13.4 SPCURITY or society in controls on an onaging basis to ensure the continued effectiveness of the controls.  3.13.4 SPCURITY or society in controls on an onaging basis to ensure the continued effectiveness are implemented, and the relationships with or connections to other systems.  3.13.3 SYSTEM                                  |  | '                 | '                 | · •   |
| tatin - though not only for Rubin so not permanently at the observatory.  3.10.3 Escort visitors and monitor visitor activity.  3.10.4 Maintain audit logs of physical access.  N Y Chie usonida key-card system, we should reach to them to inquire about their audit procedures 3.10.5 Control and manage physical access devices.  3.10.5 Control and manage physical access devices.  3.10.5 Scontrol and manage physical access devices.  Y Y This brings in NIST.800-46 and NIST.800-114. Threat analysis suggested. NAT considered bad.  3.11 RISK ASSESSMENT  3.11.1 RISK ASSESSMENT  3.11.1 Periodally assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational assets and applications are identified.  3.12.1 Scon for vulnerabilities in organizational systems and applications are identified.  3.12.2 Devologa and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.2 Devologa and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.2 Devologa document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13.3 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (Le, information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational asystems.  3.13.3 SySTEM AND COMMUNICATIONS PROTECTION  3.13.3 SySTEM (In the propose of feetive information transfer via shared system in control and communications (Le, information transfer via shared system)  3.13.3 Implem                                  | operating environments to authorized individuals.  |                   |                   | inets etc. but key card access is already in place.   |
| tatin - though not only for Rubin so not permanently at the observatory.  3.10.3 Escort visitors and monitor visitor activity.  3.10.4 Maintain audit logs of physical access.  N Y Chie usonida key-card system, we should reach to them to inquire about their audit procedures 3.10.5 Control and manage physical access devices.  3.10.5 Control and manage physical access devices.  3.10.5 Scontrol and manage physical access devices.  Y Y This brings in NIST.800-46 and NIST.800-114. Threat analysis suggested. NAT considered bad.  3.11 RISK ASSESSMENT  3.11.1 RISK ASSESSMENT  3.11.1 Periodally assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational assets and applications are identified.  3.12.1 Scon for vulnerabilities in organizational systems and applications are identified.  3.12.2 Devologa and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.2 Devologa and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.2 Devologa document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13.3 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (Le, information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational asystems.  3.13.3 SySTEM AND COMMUNICATIONS PROTECTION  3.13.3 SySTEM (In the propose of feetive information transfer via shared system in control and communications (Le, information transfer via shared system)  3.13.3 Implem                                  | 2.10.2 Protect and monitor the physical facility and support infrastructure for organi   | V                 | V                 | Socurity is in place on Core Pachon and at the entrance to the moun   |
| 3.10.3 Escort visitors and monitor visitor activity.  3.10.4 Maintain audit logs of physical access.  N Y Chile use Norlab key-card system, we should reach to them to inquire about their audit procedures  3.10.5 Enforce safeguarding measures for CUI at alternate work sites.  3.10.6 Enforce safeguarding measures for CUI at alternate work sites.  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.1 Periodically assess the risk to organizational systems and applications periodically and when new vulnerabilities in organizational systems and applications periodically and when new vulnerabilities in organizational systems and applications periodically and when new vulnerabilities in organizational systems and applications periodically and when new vulnerabilities in organizational systems and applications are identified.  3.11.2 Escolarity ASSESSMENT  3.12.5 EVEURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13.5 YSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.3 Separate user functionality from system management functionality.  3.13.3 Finglement can do not put it on their devices.  3.13.5 Implemented                                  |  | 1                 |                   | , ,   |
| 3.10.3 Escort visitors and monitor visitor activity.  3.10.4 Maintain audit logs of physical access.  N Y Chile use Norlab key-card system, we should reach to them to inquire about their audit procedures  3.10.5 Enforce safeguarding measures for CUI at alternate work sites.  3.10.6 Enforce safeguarding measures for CUI at alternate work sites.  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.1 Periodically assess the risk to organizational systems and applications periodically and when new vulnerabilities in organizational systems and applications periodically and when new vulnerabilities in organizational systems and applications periodically and when new vulnerabilities in organizational systems and applications periodically and when new vulnerabilities in organizational systems and applications are identified.  3.11.2 Escolarity ASSESSMENT  3.12.5 EVEURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13.5 YSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.3 Separate user functionality from system management functionality.  3.13.3 Finglement can do not put it on their devices.  3.13.5 Implemented                                  | zational systems.  |                   |                   | tain - though not only for Rubin so not permanently at the observa-   |
| 3.10.3 Escort visitors and monitor visitor activity.  3.10.4 Maintain audit logs of physical access.  N Y Chile use Noirlab key-card system, we should reach to them to inquire about their audit procedures  3.10.5 Control and manage physical access devices.  3.10.6 Enforce safeguarding measures for CUI at alternate work sites.  3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new ulnerabilities affecting those systems and applications are identified.  3.12.2 ScEURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and their relationships with or connections to other systems.  3.13.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.13.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and their relationships with or connections to other systems.  3.13.3 System And COMMUNICATIONS PROTECTION  3.13.4 Provent unauthorized and unintended information transfer via shared system senional systems.  3.13.3 Spearate user functionality from system management functionality.                                   |  |                   |                   | NV  |
| a. 3.10.4 Maintain audit logs of physical access.  N Y Chile use Noriab key-card system, we should reach to them to inquire about their audit procedures  3.10.5 Control and manage physical access devices.  3.10.6 Enforce safeguarding measures for CUI at alternate work sites.  Y Y This brings in NIST.800-46 and NIST.800-114. Threat analysis suggested. NAT considered bad.  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 SECURITY ASSESSMENT  3.12.1 Periodically saves the security controls in organizational systems and applications are identified.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Nonitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.13.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13.3 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.4 Prevent unauthorized and unintended information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  This is difficult in development and commissioning but should be oking periodices.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.   |  |                   |                   | tory.   |
| a. 3.10.4 Maintain audit logs of physical access.  N Y Chile use Noriab key-card system, we should reach to them to inquire about their audit procedures  3.10.5 Control and manage physical access devices.  3.10.6 Enforce safeguarding measures for CUI at alternate work sites.  Y Y This brings in NIST.800-46 and NIST.800-114. Threat analysis suggested. NAT considered bad.  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 SECURITY ASSESSMENT  3.12.1 Periodically saves the security controls in organizational systems and applications are identified.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Nonitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.13.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13.3 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.4 Prevent unauthorized and unintended information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  This is difficult in development and commissioning but should be oking periodices.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.   | 3.10.3 Escort visitors and monitor visitor activity.   | Υ                 | Y                 | Actual visitors are escorted on the summit - contractors are consid-  |
| 3.10.4 Maintain audit logs of physical access.  N   |  |                   |                   |   |
| 3.10.5 Control and manage physical access devices. 3.10.5 Control and manage physical access devices. 3.10.6 Enforce safeguarding measures for CUI at alternate work sites.  3.10.6 Enforce safeguarding measures for CUI at alternate work sites.  3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 San for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities in organizational systems and applications are identified. 3.12.2 EVEQUARD ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that desirely system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13 SYSTEM AND COMMUNICATIONS PROTECTION 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information transfer via shared system 3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  This will require training the operators and scientist who have access to the CUI data to not put it on their devices.   |  |                   |                   | ered more like staff.   |
| 3.10.5 Control and manage physical access devices. 3.10.5 Control and manage physical access devices. 3.10.6 Enforce safeguarding measures for CUI at alternate work sites.  3.10.6 Enforce safeguarding measures for CUI at alternate work sites.  3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 San for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities in organizational systems and applications are identified. 3.12.2 EVEQUARD ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that desirely system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13 SYSTEM AND COMMUNICATIONS PROTECTION 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information transfer via shared system 3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  This will require training the operators and scientist who have access to the CUI data to not put it on their devices.   | 3 10 4 Maintain audit logs of physical access  | N                 | V                 | Chile use Noirlah key-card system, we should reach to them to in-   |
| 3.10.5 Control and manage physical access devices. 3.10.6 Enforce safeguarding measures for CUI at alternate work sites. Y Y This brings in NIST.800-46 and NIST.800-114. Threat analysis suggested. NAT considered bad. 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13.3 SYSTEM AND COMMUNICATIONS PROTECTION 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. 3.13.2 Employ architectural designs, software development techniques, and systems are implemented and unintended information transfer via shared system principles that promote effective information transfer via shared system in promote effective information transfer via shared system in properations. 3.13.3 Separate user functionality from system management functionality.  N Y This will require training the operators and scientist who have acce                                  | 3.10.4 Maintain additiogs of physical access.  |                   | 1 '               |   |
| 3.10.6 Enforce safeguarding measures for CUI at alternate work sites.  3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications are identified.  3.11.2 Scan for vulnerabilities affecting those systems and applications are identified.  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Morth of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information rescurity within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.5 Implement subnetworks for publicly accessible system components that are Y   |  |                   |                   | quire about their audit procedures  |
| 3.10.6 Enforce safeguarding measures for CUI at alternate work sites.  3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications are identified.  3.11.2 Scan for vulnerabilities affecting those systems and applications are identified.  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Morth of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information rescurity within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.5 Implement subnetworks for publicly accessible system components that are Y   | 3 10 5 Control and manage physical access devices  | V                 | V                 |   |
| gested. NAT considered bad.  3.11. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12.5 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13.5 YSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems) at the external boundaries and key internal boundaries of organizational systems) at the external boundaries and key internal boundaries of prognalizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  This is difficult in development and commissioning but should be ok in operations.  3.13.5 Implement subnetworks for publicly accessible system components that are V   |  |                   |                   |   |
| 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities affecting those systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12.5 ECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. 3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  This is difficult in development and commissioning but should be ok in operations. 3.13.4 Prevent unauthorized and unintended information transfer via shared system on the CUI data to not put it on their devices. 3.13.5 Implements subnetworks for publicly accessible system components that are V   | 3.10.6 Enforce safeguarding measures for CIII at alternate work sites  | Υ                 | l y               | This brings in NIST.800-46 and NIST.800-114. Threat analysis sug-   |
| 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities affecting those systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12.5 ECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. 3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  This is difficult in development and commissioning but should be ok in operations. 3.13.4 Prevent unauthorized and unintended information transfer via shared system on the CUI data to not put it on their devices. 3.13.5 Implements subnetworks for publicly accessible system components that are V   |  |                   |                   |   |
| 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities in organizational systems and applications periodically and when new vulnerabilities in organizational systems and applications are identified. 3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13.3 SYSTEM AND COMMUNICATIONS PROTECTION 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. 3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  This is difficult in development and commissioning but should be ok in operations. 3.13.4 Prevent unauthorized and unintended information transfer via shared system or your proposed propagation of the pr                                  | Stroto Emoree sureguarding measures for eor at alternate work sites.   |                   |                   | gested NAT considered had   |
| functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12.2 EVECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.11.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. 3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  We can do more here.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.   |  |                   |                   | gested. NAT considered bad.   |
| functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12.2 EVECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.11.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. 3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  We can do more here.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.   |  |                   | <u> </u>          | gested. NAT considered bad.   |
| the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12.5 ESCURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effective-tiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are V  | 3.11 RISK ASSESSMENT   | V                 |                   | gested. NAT considered bad.   |
| the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12.5 ESCURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effective-tiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are V  | 3.11 RISK ASSESSMENT     3.11.1 Periodically assess the risk to organizational operations (including mission,  | Y                 |                   | gested. NAT considered bad.   |
| transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Separate user functionality from system management functionality.  3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are   | 3.11 RISK ASSESSMENT     3.11.1 Periodically assess the risk to organizational operations (including mission,  | Y                 |                   | gested. NAT considered bad.   |
| 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effective ensures of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are Y  | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from  | Y                 |                   | gested. NAT considered bad.   |
| 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effective ensures of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are Y  | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from  | Y                 |                   | gested. NAT considered bad.   |
| and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are  Y  Y  This will require training the operators and scientist who have access to the CUI data to not put it on their devices.  | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or   | Y                 |                   | gested. NAT considered bad.   |
| 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13 SYSTEM AND COMMUNICATIONS PROTECTION 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. 3.13.3 Separate user functionality from system management functionality.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources. 3.13.5 Implement subnetworks for publicly accessible system components that are resources. 3.13.5 Implement subnetworks for publicly accessible system components that are resources.  | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  |                   | Y                 |   |
| 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13 SYSTEM AND COMMUNICATIONS PROTECTION 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. 3.13.3 Separate user functionality from system management functionality.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources. 3.13.5 Implement subnetworks for publicly accessible system components that are resources. 3.13.5 Implement subnetworks for publicly accessible system components that are resources.  | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  |                   | Y                 |   |
| 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effective inveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are Y  | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically   |                   | Y                 |   |
| if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13.5YSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  Y Y We can do more here.  This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are Y   | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.   |                   | Y                 |   |
| if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13.5YSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  Y Y We can do more here.  This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are Y   | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.   |                   | Y                 |   |
| 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  3.13.4 Prevent unauthorized and unintended information transfer via shared system  3.13.5 Implement subnetworks for publicly accessible system components that are  Y  Y  Y  We can do more here.  Y  This is difficult in development and commissioning but should be ok in operations.  Y  This will require training the operators and scientist who have access to the CUI data to not put it on their devices.  | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT  | N                 | Y                 |   |
| reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are  Y Y   | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine  | N                 | Y                 |   |
| reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are  Y Y   | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine  | N                 | Y                 |   |
| 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are  Y Y  | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  | N<br>Y            | Y                 |   |
| tiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.   | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and   | N<br>Y            | Y                 |   |
| tiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.   | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and   | N<br>Y            | Y                 |   |
| 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y We can do more here.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are  Y Y  | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  | N Y Y             | Y                 |   |
| scribe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.   | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effec-   | N Y Y             | Y                 |   |
| scribe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.   | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effec-   | N Y Y             | Y                 |   |
| ments are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.   | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.   | N<br>Y<br>Y       | Y                 | Third party contract  |
| 3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.   | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that de-  | N<br>Y<br>Y       | Y                 | Third party contract  Like any documentation this security documentation can get out of   |
| 3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.   | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that de-  | N<br>Y<br>Y       | Y                 | Third party contract  Like any documentation this security documentation can get out of   |
| 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.  | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security require-  | N<br>Y<br>Y       | Y                 | Third party contract  Like any documentation this security documentation can get out of   |
| 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.  | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  | N<br>Y<br>Y       | Y                 | Third party contract  Like any documentation this security documentation can get out of   |
| or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.   | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  | N<br>Y<br>Y       | Y                 | Third party contract  Like any documentation this security documentation can get out of   |
| boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.  | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  | N Y Y Y N         | Y Y Y Y Y         | Third party contract  Like any documentation this security documentation can get out of   |
| boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.  | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted)  | N Y Y Y N         | Y Y Y Y Y         | Third party contract  Like any documentation this security documentation can get out of   |
| 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are Y Y  | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted)  | N Y Y Y N         | Y Y Y Y Y         | Third party contract  Like any documentation this security documentation can get out of   |
| engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.  3.13.5 Implement subnetworks for publicly accessible system components that are Y Y  | 3.11 RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal  | N Y Y Y N         | Y Y Y Y Y         | Third party contract  Like any documentation this security documentation can get out of   |
| engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.  3.13.5 Implement subnetworks for publicly accessible system components that are Y Y  | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13 SYSTEM AND COMMUNICATIONS PROTECTION 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.   | N Y Y Y N         | Y Y Y Y Y Y       | Third party contract  Like any documentation this security documentation can get out of   |
| tional systems.  3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.  3.13.5 Implement subnetworks for publicly accessible system components that are Y Y  | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13 SYSTEM AND COMMUNICATIONS PROTECTION 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.   | Y Y Y N           | Y Y Y Y Y Y       | Third party contract  Like any documentation this security documentation can get out of date.   |
| 3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.  3.13.5 Implement subnetworks for publicly accessible system components that are Y Y   | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13 SYSTEM AND COMMUNICATIONS PROTECTION 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. 3.13.2 Employ architectural designs, software development techniques, and systems   | Y Y Y N           | Y Y Y Y Y Y       | Third party contract  Like any documentation this security documentation can get out of date.   |
| 3.13.3 Separate user functionality from system management functionality.  N Y This is difficult in development and commissioning but should be ok in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.  3.13.5 Implement subnetworks for publicly accessible system components that are Y Y   | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13 SYSTEM AND COMMUNICATIONS PROTECTION 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. 3.13.2 Employ architectural designs, software development techniques, and systems   | Y Y Y N           | Y Y Y Y Y Y       | Third party contract  Like any documentation this security documentation can get out of date.   |
| in operations.  3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  3.13.5 Implement subnetworks for publicly accessible system components that are Y Y Y   | 3.11 RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13 SYSTEM AND COMMUNICATIONS PROTECTION 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organiza-   | Y Y Y N           | Y Y Y Y Y Y       | Third party contract  Like any documentation this security documentation can get out of date.   |
| 3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.  N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.  3.13.5 Implement subnetworks for publicly accessible system components that are Y Y   | 3.11. RISK ASSESSMENT  3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems) at the external boundaries and key internal boundaries of prognizational systems.   | N Y Y Y Y N Y     | Y Y Y Y Y Y Y     | Third party contract  Like any documentation this security documentation can get out of date.  We can do more here.   |
| 3.13.4 Prevent unauthorized and unintended information transfer via shared system N Y This will require training the operators and scientist who have access to the CUI data to not put it on their devices.  3.13.5 Implement subnetworks for publicly accessible system components that are Y Y   | 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems) at the external boundaries and key internal boundaries of prognizational systems.  | N Y Y Y Y N Y     | Y Y Y Y Y Y Y     | Third party contract  Like any documentation this security documentation can get out of date.  We can do more here.   |
| resources. to the CUI data to not put it on their devices.  3.13.5 Implement subnetworks for publicly accessible system components that are Y Y   | 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems) at the external boundaries and key internal boundaries of prognizational systems.  | N Y Y Y Y N Y     | Y Y Y Y Y Y Y     | Third party contract  Like any documentation this security documentation can get out of date.  We can do more here.  This is difficult in development and commissioning but should be ok  |
| resources. to the CUI data to not put it on their devices.  3.13.5 Implement subnetworks for publicly accessible system components that are Y Y   | 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.   | N Y Y Y N N N     | Y Y Y Y Y Y Y     | Third party contract  Like any documentation this security documentation can get out of date.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.   |
| 3.13.5 Implement subnetworks for publicly accessible system components that are Y Y   | 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.   | N Y Y Y N N N     | Y Y Y Y Y Y Y     | Third party contract  Like any documentation this security documentation can get out of date.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.   |
|   | 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.             | N Y Y Y N N N     | Y Y Y Y Y Y Y     | Third party contract  Like any documentation this security documentation can get out of date.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.  This will require training the operators and scientist who have access |
|   | 3.11. RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13 SYSTEM AND COMMUNICATIONS PROTECTION 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. 3.13.3 Separate user functionality from system management functionality. | Y Y Y N Y Y N N N | Y Y Y Y Y Y Y Y Y | Third party contract  Like any documentation this security documentation can get out of date.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.  This will require training the operators and scientist who have access |
| priyoraniy or rogicany ocparated from internal networks.  | 3.11. RISK ASSESSMENT 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.12 SECURITY ASSESSMENT 3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 3.13 SYSTEM AND COMMUNICATIONS PROTECTION 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. 3.13.3 Separate user functionality from system management functionality. | Y Y Y N Y Y N N N | Y Y Y Y Y Y Y Y Y | Third party contract  Like any documentation this security documentation can get out of date.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.  This will require training the operators and scientist who have access |
|   | 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.  3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.12 SECURITY ASSESSMENT  3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  3.13.3 Separate user functionality from system management functionality.             | Y Y Y N Y Y N N N | Y Y Y Y Y Y Y Y Y | Third party contract  Like any documentation this security documentation can get out of date.  We can do more here.  This is difficult in development and commissioning but should be ok in operations.  This will require training the operators and scientist who have access |

DRAFT 12 DRAFT



| 3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). | Y | Y   | We may need to bring up iptables on each host    |
|--|---|-----|--|
| 3.13.7 Prevent remote devices from simultaneously establishing non-remote connec-  | Υ | Y   |  |
| tions with organizational systems and communicating via some other connection to   |   |     |  |
| resources in external networks (i.e., split tunneling).  |   |     |  |
| 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of  | N | Y   | IPSec and encryption coming                      |
| CUI during transmission unless otherwise protected by alternative physical safe-   |   |     |  |
| guards.  |   |     |  |
| 3.13.9 Terminate network connections associated with communications sessions at  | Υ | Y   |  |
| the end of the sessions or after a defined period of inactivity.   |   |     |  |
| 3.13.10 Establish and manage cryptographic keys for cryptography employed in or-   | Υ | Y   |  |
| ganizational systems.  |   |     |  |
| 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality  | N | Y   |  |
| of CUI.  |   |     |  |
| 3.13.12 Prohibit remote activation of collaborative computing devices and provide  | Υ | Y   | We should take care with the new roaming camera. |
| indication of devices in use to users present at the device.   |   |     |  |
| 3.13.13 Control and monitor the use of mobile code.  | Υ | Υ   | Currently we have no mobile code                 |
| 3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technolo-   | N | Y   | Chile dont monitor voip callls                   |
| gies.  |   |     |  |
| 3.13.15 Protect the authenticity of communications sessions.   | Υ | Υ   |  |
| 3.13.16 Protect the confidentiality of CUI at rest.  | N | Υ   |  |
| 3.14 SYSTEM AND INFORMATION INTEGRITY  |   |     |  |
| 3.14.1 Identify, report, and correct system flaws in a timely manner.  | Υ | Υ   |  |
| 3.14.2 Provide protection from malicious code at designated locations within organi-   | Υ | Y   |  |
| zational systems.  |   |     |  |
| 3.14.3 Monitor system security alerts and advisories and take action in response.  | Υ | Υ   |  |
| 3.14.4 Update malicious code protection mechanisms when new releases are avail-  | Υ | Υ   |  |
| able.  |   |     |  |
| 3.14.5 Perform periodic scans of organizational systems and real-time scans of files   | Υ | Υ   |  |
| from external sources as files are downloaded, opened, or executed.  |   |     |  |
| 3.14.6 Monitor organizational systems, including inbound and outbound communi-   | Υ | Υ   |  |
| cations traffic, to detect attacks and indicators of potential attacks.  |   |     |  |
| Total requirements   |   | 108 |  |
| Total Rubin Intends to comply with   |   | 108 |  |
| Total Rubin Complies with in 2021  |   | 72  |  |

DRAFT 13 DRAFT



#### **B** References

- [SQR-037], Allbery, R., 2020, SQuaRE security risk assessment, SQR-037, URL https://sqr-037.lsst.io/
- [SQR-041], Allbery, R., 2021, Science Platform security risk assessment, SQR-041, URL https://sqr-041.lsst.io/
- **[LSE-30]**, Claver, C.F., The LSST Systems Engineering Integrated Project Team, 2018, *Observatory System Specifications (OSS)*, LSE-30, URL https://ls.st/LSE-30
- [NIST.FIPS.200], Division, C.S., 2006, Publication 200, minimum security requirements for federal information and information systems, URL https://doi.org/10.6028/NIST.FIPS.200
- [ITTN-014], Gonzalez, I., 2021, *Computing Infrastructure*, ITTN-014, URL https://ittn-014.lsst.io/
- [LDM-324], Kantor, J., 2016, *Data Management Information Security Plan*, LDM-324, URL https://ls.st/LDM-324
- [DMTN-108], O'Mullane, W., 2021, Security of Rubin Observatory data, DMTN-108, URL https://dmtn-108.lsst.io/
- [DMTN-135], O'Mullane, W., Dubois, R., Butler, M., Lim, K.T., 2021, *DM sizing model and cost plan for construction and operations.*, DMTN-135, URL https://dmtn-135.lsst.io/
- [NIST.SP.800-171], ROSS, R., VISCUSO, P., GUISSANIE, G., DEMPSEY, K., RIDDLE, M., 2020, Special publication 800-171, protecting controlled unclassified information in nonfederal systems and organizations, URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
- [NIST.800-114], Souppaya, M., Scarfone, K., 2016, COMPUTER SECURITY, URL https://doi. org/10.6028/NIST.SP.800-114r1
- [NIST.800-46], Souppaya, M., Scarfone, K., 2016, COMPUTER SECURITY, URL https://doi.org/ 10.6028/NIST.SP.800-46r2

DRAFT 14 DRAFT



# C Acronyms



DRAFT 15 DRAFT



| Acronym | Description  |
|---------|--|
| AES     | Advanced Encryption Standard   |
| AURA    | Association of Universities for Research in Astronomy                    |
| AVS     | Alert Vetting System   |
| CPU     | Central Processing Unit  |
| CUI     | Controlled Unclassified Information                                      |
| ComCam  | The commissioning camera is a single-raft, 9-CCD camera that will be in- |
|         | stalled in LSST during commissioning, before the final camera is ready.  |
| DM      | Data Management  |
| DMTN    | DM Technical Note  |
| DOE     | Department of Energy   |
| FIPS    | Federal Information Processing Standards                                 |
| FIU     | Florida International University   |
| FTE     | Full-Time Equivalent   |
| IPsec   | Internet Protocol Security   |
| IRU     | indefinable right to use   |
| IT      | Information Technology   |
| JSR     | Joint Status Review  |
| LDM     | LSST Data Management (Document Handle)                                   |
| LHN     | long haul network  |
| LLNL    | Lawrence Livermore National Laboratory                                   |
| LSE     | LSST Systems Engineering (Document Handle)                               |
| NAT     | Network Address Translation  |
| NCSA    | National Center for Supercomputing Applications                          |
| NIST    | National Institute of Standards and Technology (USA)                     |
| NSF     | National Science Foundation  |
| OGA     | Other Government Agencies  |
| ООВ     | Out Of Bound (Alternative network access)                                |
| OSS     | Observatory System Specifications; LSE-30                                |
| RAID    | Redundant Array of Inexpensive Disks                                     |
| ROP     | Rubin Operations Plan  |
| RSP     | Rubin Science Platform   |
| SATA    | Serial Advanced Technology Attachment                                    |
| SLAC    | SLAC National Accelerator Laboratory                                     |

DRAFT 16 DRAFT



| SOC  | Security Operations Centre  |
|------|-----------------------------|
| SQR  | SQuARE document handle      |
| SSD  | Solid-State Disk            |
| ТВ   | TeraByte                    |
| TLS  | Transport Layer Security    |
| USDF | United States Data Facility |
| VPN  | virtual private network     |
| deg  | degree; unit of angle       |
|      |                             |

DRAFT 17 DRAFT