

Vera C. Rubin Observatory Data Management

CUI Rubin Observatory Data Security Standards Response

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

DMTN-199

Latest Revision: 2021-07-20





Abstract

This is a response to the Controlled Unclassified Information (CUI) document from the agencies.



Change Record

Version	Date	Description	Owner name
0.1	2021-07-19	Unreleased. Set up structure	William O'Mullane

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



Contents

1	Introduction	1
2	Cost Summary	2
3	Response to the requirements	2
	3.1 Encrypt Data	2
	3.2 Install Firewalls	3
	3.3 Delay public release	3
	3.4 Eliminate earth orbiting satellites	3
	3.5 Perform earth orbiting satellite processing in separate facility	3
	3.6 Publish nominal schedule	3
	3.7 Request approval for non sidereal tracking	3
4	Conclusion	3
Α	Compliance with NIST Standard	3
В	References	7
C	Acronyms	7



CUI Rubin Observatory Data Security Standards Response

1 Introduction

The agencies have provided a set of requirements for security which we asses here and provide initial cost impact analysis for.

The summary requirements (from the start of the document) are:

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

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



2 Cost Summary

Costs are detailed in each section below Table 1 gives a summary.

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

Encryption	\$3,204,000.00
Total	\$3,204,000.00

3 Response to the requirements

There is an implication that we should follow NIST.SP.800-171, as for any standard that is open to some interpretation. We will have to show how we comply to the standard. This may take the form of a compliance matrix as shown in Appendix A. In this matrix and in this document we assume CUI refers to embargoed images before release to the collaboration.

We assume this applies to CUI, which we interpret as the embargoed image data hence it applies to Prompt Processing, the embargoed data store(s) and the summit in Chile. It does snot apply to DACs nor the actual alert stream.

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

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

3.1 Encrypt Data

As outlined in ? we propose to buy fuor routers which can perform AES IPSec 256 bit encryption between Chile and SLAC. We will not transfer embargoed images to France - hence we should keep an secure data store at Chile and at SLAC for redundancy.

See Table 2 for the cost breakdown.

¹{confidentiality, availability,integrity}



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

Item	Cost	number	Total
Cisco Router	\$800,000.00	4	\$3,200,000.00
Cabeling	\$1,000.00	4	\$4,000.00
Misc			
Total			\$3,204,000.00

3.2 Install Firewalls

3.3 Delay public release

3.4 Eliminate earth orbiting satellites

3.5 Perform earth orbiting satellite processing in separate facility

3.6 Publish nominal schedule

3.7 Request approval for non sidereal tracking

4 Conclusion

A Compliance with NIST Standard

Table 3: This table provides an overview of the NIST.SP.800-171 and Rubin compliance with it.

NIST 800-171	2021	Intended	Note
	Status	Compli-	
		ance	
3.1 ACCESS CONTROL			
3.1.1 Limit system access to authorized users, processes acting on behalf of 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.	Y	Y	
3.1.3 Control the flow of CUI in accordance with approved authorizations.	Y	Y	
3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity with-	Υ	Y	Principle of least privilage is applied.
out collusion.			
3.1.5 Employ the principle of least privilege, including for specific security functions	Υ	Υ	
and privileged accounts.			
3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.	Υ	Υ	
3.1.7 Prevent non-privileged users from executing privileged functions and capture		Y	Cristian Richard - does this include SUDO ?
the execution of such functions in audit logs.			
3.1.8 Limit unsuccessful logon attempts.	N	Υ	I dont belive we do this now but we can
3.1.9 Provide privacy and security notices consistent with applicable CUI rules.	N	Y	Check login notices etc.
3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of	Υ	Υ	This is our policy.
data after a period of inactivity.			
3.1.11 Terminate (automatically) a user session after a defined condition.	Υ	Υ	
3.1.12 Monitor and control remote access sessions.		Υ	Cristian - not sure if we do this now



3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Υ	Y	VPN is in use
3.1.14 Route remote access via managed access control points.	Υ	Y	Bastion nodes
3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.	Y	Y	Baston nodes
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.	Y	Y	
3.1.18 Control connection of mobile devices.	Y	Y	In the sense there is no open wifi, and on the summit devices must be registered.
3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.23	Y	Y	CUI will not exist on mibile devices - in the case where an image may exist on say comissioning team laptop we will have disk encruption enabled.
3.1.20 Verify and controllimit connections to and use of external systems.	Y	Y	This implies vetting of devices that connect to the control network - we use mac address for laptops and personal mobile phones can not connect to the control network.
3.1.21 Limit use of portable storage devices on external systems.	N	Y	CristianRichard - impliesn no USB drives etc enabled
3.1.22 Control CUI posted or processed on publicly accessible systems.	Υ	Y	We do not intend to post CUI on publicly accessible systems.
3.2 AWARENESS AND TRAINING			
3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the			
applicable policies, standards, and procedures related to the security of those systems.			
3.2.2 Ensure that personnel are trained to carry out their assigned information			
security-related duties and responsibilities. 3.2.3 Provide security awareness training on recognizing and reporting potential in-			
dicators of insider threat.			
3.3 AUDIT AND ACCOUNTABILITY			
3.3.1 Create and retain system audit logs and records to the extent needed to enable			
the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.			
3.3.2 Ensure that the actions of individual system users can be uniquely traced to			
those users, so they can be held accountable for their actions.			
3.3.3 Review and update logged events.			
3.3.4 Alert in the event of an audit logging process failure.			
3.3.5 Correlate audit record review, analysis, and reporting processes for investigation			
and response to indications of unlawful, unauthorized, suspicious, or unusual activity.			
3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.			
3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.			
3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.			
3.3.9 Limit management of audit logging functionality to a subset of privileged users.			
3.4 CONFIGURATION MANAGEMENT			
3.4.1 Establish and maintain baseline configurations and inventories of organizational			
systems (including hardware, software, firmware, and documentation) throughout			
the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology			
products employed in organizational systems.			
3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.			
3.4.4 Analyze the security impact of changes prior to implementation.		1	
3.4.5 Define, document, approve, and enforce physical and logical access restrictions			
associated with changes to organizational systems.			
3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.			
3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports,			
protocols, and services.			
3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution			
of authorized software.			
3.4.9 Control and monitor user-installed software.		+	
3.5 IDENTIFICATION AND AUTHENTICATION			
3.5.1 Identify system users, processes acting on behalf of users, and devices.			



Common device identifiers include Media Access Control (MAC), Internet Protocol (IP)	
addresses, or device-unique token identifiers. Management of individual identifiers	
is not applicable to shared system accounts. Typically, individual identifiers are the	
user names associated with the system accounts assigned to those individuals. Or-	
ganizations may require unique identification of individuals in group accounts or for	
detailed accountability of individual activity. In addition, this requirement addresses	
individual identifiers that are not necessarily associated with system accounts. Orga-	
nizational devices requiring identification may be defined by type, by device, or by a	
combination of typedevice.	
3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a pre-	
requisite to allowing access to organizational systems.	
3.5.3 Use multifactor authentication for local and network access to privileged ac-	
counts and for network access to non-privileged accounts.24 25	
3.5.4 Employ replay-resistant authentication mechanisms for network access to priv-	
ileged and non- privileged accounts.	
3.5.5 Prevent reuse of identifiers for a defined period.	
3.5.6 Disable identifiers after a defined period of inactivity.	
3.5.7 Enforce a minimum password complexity and change of characters when new	
passwords are created.	
•	
3.5.8 Prohibit password reuse for a specified number of generations.	
3.5.9 Allow temporary password use for system logons with an immediate change to	
a permanent password.	
3.5.10 Store and transmit only cryptographically-protected passwords.	
7 71 0 1 71	
3.5.11 Obscure feedback of authentication information.	
3.6 INCIDENT RESPONSE	
3.6.1 Establish an operational incident-handling capability for organizational systems	
that includes preparation, detection, analysis, containment, recovery, and user re-	
sponse activities.	
3.6.2 Track, document, and report incidents to designated officials andor authorities	
both internal and external to the organization.	
3.6.3 Test the organizational incident response capability.	
3.7 MAINTENANCE	
3.7.1 Perform maintenance on organizational systems.26	
3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to	
conduct system maintenance.	
3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.	
3.7.4 Check media containing diagnostic and test programs for malicious code before	
the media are used in organizational systems.	
3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions	
3.7.3 Require multifactor authentication to establish nomocal maintenance sessions	
via external network connections and terminate such connections when nonlocal	
via external network connections and terminate such connections when nonlocal maintenance is complete.	
maintenance is complete.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without re-	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI. 3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI. 3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI. 3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. 3.10 PHYSICAL PROTECTION 3.10.1 Limit physical access to organizational systems, equipment, and the respective	
maintenance is complete. 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 3.8 MEDIA PROTECTION 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse. 3.8.4 Mark media with necessary CUI markings and distribution limitations.27 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 3.8.7 Control the use of removable media on system components. 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 3.8.9 Protect the confidentiality of backup CUI at storage locations. 3.9 PERSONNEL SECURITY 3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI. 3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	



2.10.2 Protect and monitor the physical facility and support infrastructure for organizational options. 2.10.3 Secret violents and monitor desiration activity. 2.10.3 Economic and manage physical activities. 2.10.6 Economic and manage physical activities activities. 2.10.7 Economic and manage physical activities activities. 2.10.7 Economic activities. 2.10.8 Economic activities. 2.10.8 Economic activities. 2.10.8 Economic activities. 2.10.8 Economic activities. 2.10.9 Economic activities. 2.10.9 Economic activities. 2.10.9 Economic activities. 2.10.1 Economic			
310.10 Second value and monitor valour activity. 310.10 Almanian and tips of physical access devices. 310.10 Almanian and tips of physical access devices. 310.10 Enforce subgrading measures for citil an attenuare work sites. 311.10 Enforce subgrading measures for citil an attenuare work sites. 311.10 Enforce subgrading measures for citil an attenuare work sites. 311.10 Enforce subgrading measures for citil an attenuare work sites. 311.10 Enforce subgrading measures for citil an attenuare work sites. 311.10 Enforce subgrading measures for citil an attenuare work sites. 311.10 Enforce subgrading measures for citil an attenuare work sites. 311.10 Enforce subgrading measures for citil and the associated possessing, along or citil and citil	3.10.2 Protect and monitor the physical facility and support infrastructure for organi-		
3.10.4 Emergency and analysis of the control of the control of the control. 3.10.5 Control and implement glance of the control of the control. 3.10.5 Employably assess the recommendation of the control of the control. 3.10.5 Employably assess the recommendation of the control of the cont	zational systems.		
3.10.5 Control and manage physical access devices. 3.11 BRIA SASSESMENT 3.11 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation) organizational operations (including mission, functions, image, or reputation) organizational speese, and individuals, resulting from the operation of operations in organizational speese, and individuals, resulting from the operation of operational individuals and the associated processing, storage, or an accessing the operation of operations and individuals of the operation of operations or an individual organizational speems and applications periodically and when new unlendlines affecting loss systems and applications periodically and when new unlendlines affecting loss systems and applications periodically and when new unlendlines affecting loss systems and applications are identified. 3.13 ENGINETY ASSESSMENT 3.12 Periodically implement pains or sicinal resigned to correct deficiencies and reduce or eliminate subtra-rebilities in organizational systems. 3.12.1 Periodically implement pains or sicinal resigned to correct deficiencies and reduce or eliminate subtra-rebilities in organizational systems. 3.12.2 Develop, document, and periodically update systems security plans that decide the security of the operation of the security requirements are implemented, and the relationships with or connections to other systems systems are implemented, and the relationships with or connections to other systems. 3.13.3 Monitor, corrol, and protect communications (i.e., information transmitted boundaries of organizational systems. 3.13.2 Employ activities of the systems or some development extending and systems engineering principles that promote effective information security within organizational systems. 3.13.3 Periodic control and security and systems are observed to a control of the system organization and systems. 3.13.3 Periodic control and security of the system security within organizational systems and understood or o	3.10.3 Escort visitors and monitor visitor activity.		
3.10.E Prioritizedly assess the risk to organizational operations (including mission, curricution, image, or reputation), organizational operations (including mission, curricution, image, or reputation), organizational assess, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 2.12.Environment of the control	3.10.4 Maintain audit logs of physical access.		
3.11 SPEND AND COMMANIACTION PROTECTION 3.13 September of the company of the control of the company of the comp	3.10.5 Control and manage physical access devices.		
3.11 SPEND AND COMMANIACTION PROTECTION 3.13 September of the company of the control of the company of the comp	3.10.6 Enforce safeguarding measures for CUI at alternate work sites.		
3.11.1 Periodically assess the risk to organizational operations (including rision), throughout the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.3 Soan fire valuerabilities in organizational systems and applications periodically and when the value distillates affecting those systems and applications are identified. 3.11.2 Invalidating assess the excurtly controls in organizational systems and applications are identified. 3.11.2 Invalidating assess the excurtly controls in organizational systems to determine if the cortical are defective in other application. 3.12.2 Develop and implement plans of action designed to correct deficienches and reduce or eliminate vulnerabilities in organizational systems. 3.12.3 Ministra security controls on an ongoing basis to ensure the continued effect organization value in the controls. 3.12.4 Develop, document, and periodically update system security plans that de-scribe system boundaries, system environments of operation, how security requirements are implemented, and the relationships when or connections to other systems boundaries, system environments of operation, how security requirements of repetition of the relationships when or connections to other systems are understanding and the relationships when or connections to other systems are understanding and the relationships when or connections to other systems are understanding and the relationships when or connections to other systems are included and unintended information transmitted or released by organizational systems, in the case of the control of the production of the control of the control of the relationships when organizational systems, control, and product communications are also systems and control of the control of the production of the control of the co			
functions, image, or reputation), organizational sesses, and individuals reading from the operation of organizational systems and the associated processing, storage, or transmission of CUI. 3.11.2 Sean for vulnerabilities in organizational systems and applications periodically and when new valuerabilities all foreign those systems and applications are identified. 3.12.1 Periodically assess the scurling those systems and applications are identified. 3.12.2 Periodically assess the scurling process of the control of programma and periodically and values in expensive systems and applications are identified. 3.12.2 Develops and implement plans or adion designed to correct defidencies and reduce or eliminate wilnerabilities in organizational systems. 3.12.2 Develops accuring ordanization and against a considerabilities of the controls. 3.12.4 Develops country corrects on an angoing basis to ensure the continued effect thereses of the controls. 3.12.4 Develops country and periodically update system security plans that desorties system boundaries, system environments of operations, how security requirements are implemented, and the reliaborability with or connections to other systems. 32 3.13.24 Develops colorations are supported to the systems and the security of the systems. 32 3.13.3 Systems and the system of the section of boundaries and key internal boundaries of regimental development of the systems. 3.13.3 Employ with tectural designs, software development exhibitions, and systems are graphy varieticitural designs, software development exhibitions, and systems are graphy varieticitural designs, software development exhibition or particitural process of the control of the section of the process of the control of the systems. 3.13.3 Employment substitutionally given and communication of regiments and revisit (e.g., software development exhibition or particitural process of the end of the sections of the process of			
the operation of organizational systems and the associated processing, storage, or transmission of USII. 3.11.2 Earn for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities offering those systems and applications are identified. 3.12.3 EURIPH ASSESSMENT. 3.12.12 Periodically assess the security controls in organizational systems to determine if the corrols are effective in their application. 3.12.2 Develop and implement plans of action designed to correct deficiencies and implement plans or against a management of the correct deficiencies and applications or against the state of the control of the correct deficiencies and applications or against the control of the correct deficiencies and applications or against the correct ordinary against the correct ordin			
It anominos not CLI. 3.1.1 2 Scan for vulnerabilities in organizational systems and applications periodically and when new-vulnerabilities is organizational systems and applications are identified. 3.1.2 1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.1.2 1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.1.2 2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.1.2 3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the curtoriols. 3.1.2 4 Develop, occurrence and periodically update system security plans that discusses a properties. In the relationships with or connections to other type terms and the relationships with or connections to other type terms. 3.1.3 13 SYSTEM AND COMMUNICATIONS PRICECTION 3.1.3.1 SYSTEM AND COMMUNICATIONS PRICECTION 3.1.3.1 Employ and protect communications (i.e., information transmitted or received by organizational systems RTDECTION and the control of the protect communications (i.e., information transmitted or received by organizational systems at the extension and protect communications (i.e., information transmitted or received by organizational systems at the extension and protect communications (i.e., information transmitted or received by organizational systems at the extension of the protect communications (i.e., information transfer via shared system controls). 3.1.3.1 Prevent remote discose of effective information security within organizational systems. 3.1.3.3 Prevent remote discose of morning and allows network communications and protect communications and an extension or anomal environment of the protect of the prot			
3.11.2 Sear for vulnerabilities in organizational systems and applications are identified. 3.12 SEURITY ASSESSMENT 3.12 Fendically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12 SEURITY ASSESSMENT 3.12 Fendically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12 Develop and implement plans or action designed to correct deficiencies and reduce or eliminate witherabilities in organizational systems. 3.12 Develops and implement plans or action designed to correct deficiencies and reduce or eliminate witherabilities in organizational systems. 3.13 Senting and periodically update nystem security plans that developed the correct controls of the corrols. 3.13 Senting and the relationships with or connections to other systems. 3.13 Senting and the relationships with or connections to other systems. 3.13.14 Monitor, control, and protect communications cell-information transmitted or received by organizational systems at the external boundaries and key internal boundaries or agreed by organizational systems. 3.13.2 Fengine virtual control, and protect communications cell-information transmitted or received by organizational systems at the external boundaries and systems. 3.13.2 Fengine virtual control, and protect communications security within organizational systems. 3.13.3 Sengine use of functionality from system management functionality. 3.13.3 Sengine use of functionality from system management functionality. 3.13.3 Sengine use of functionality from system management functionality. 3.13.3 Fengine use of functionality from system management functionality. 3.13.4 Development of the systems of the systems of the systems of the systems. 3.13.5 Prevent remote office the produce of the systems of the systems of the systems of the systems of the systems. 3.13.6 Development of the systems of the syste			
and when new-uninerabilities affecting those systems and applications are identified. 3.12 FEORITY SESSEMENT 3.12 FOORITY SESSEMENT 3.12 Prenotically assess the security controls in organizational systems to determine if the controls are effective in their application. 3.12 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.13 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.14 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.15 Monitor security controls and periodically update system security plans that describe systems development and the relationships with or connections to other systems are implemented, and the relationships with or connections to other systems are implemented. 3.13 SYSTEM AND COMMUNICATIONS POTECTION 3.13.14 SYSTEM AND COMMUNICATIONS POTECTION 3.13.15 ENDIFFICATION SECURITY SECURIT			
3.12 Ferbording asses the security controls in organizational systems. 3.12 Perbording asses the security controls in organizational systems. 3.12 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. 3.12 Monotros country controls on an organizational systems. 3.12 Monotros country controls on an organizational systems. 3.12 Monotros country controls on an organizational 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 System AND COMMUNICATIONS PROTECTION 3.13.1 Monotro, cortrol, and protect communications (i.e., information transmitted or received by organizational systems at the external boundaries and key internal boundaries of organizational systems as the external boundaries and key internal boundaries of organizational systems of the external boundaries and key internal boundaries of organizational systems and systems. 3.13.2 Employ an internal elements of the external boundaries and key internal boundaries of organizational systems and systems. 3.13.2 Employ an internal elements of the external boundaries and key internal boundaries of organizational systems and systems. 3.13.3 Expraise user functionally from system management functionality. 3.13.4 Expraise user functionality from system management functionality. 3.13.5 Expraise user functionality from system management functionality. 3.13.6 Expraise user functionality from system management functionality. 3.13.7 Expraise transmit subnetworks for publi			
3.12.1 Prioridially assess the security controls in organizational systems. 3.12.2 Develop and implement plans of action designed to correct deficiencies and recute or eliminate winerabilities 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 emicroinments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 28 3.13.3 STEM AND COMMUNICATIONS PROTECTION 3.13.14 Monitor, correct, and protect communications (i.e., information transmitted or received by organizational systems at the external boundaries and key internal boundaries or spread protection of the systems. 28 3.13.3 Stephanol systems and stephanol systems and several boundaries and key internal boundaries or principal state promote effective information security within organizational systems. 3.13.3 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 Separate user functionality from system management functionality. 3.13.5 Prevent unauthorized and unintended information transfer via shared system resources. 3.13.5 Implement subnetworks for publicly accessible system components that are physically or legislary separated from internal networks. 3.13.6 Delay network communications traffic by default and allow network communications traffic by exception it. e. deliy is permit by exception it. 3.13.6 Prevent renote devices from simultaneously esoblishing non-remote connection to the section it. e. deliy is permit by exception it. 3.13.7 Prevent renote devices from simultaneously esoblishing non-remote connection to the section of t	<u> </u>		
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 Montors control. 3.12.4 Develop o Socument, 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. 28 3.13.5 System NAN COMMUNICATIONS PROTECTION 3.13.1 Montor, control, and protect communications (i.e., information transmitted or received by organizational systems and the extention bundaries and key internal boundaries of organizational systems at the extention bundaries and key internal boundaries of organizational systems at the extention bundaries 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 System such functionality from system management functionality. 3.13.4 Prevent unauthorized and unitended information artserf via sharted system resources. 3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.6 Deep newtone devices from sumitaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in extend devices from sumitaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in extend edvelocs from sumitaneously establishing non-remote connections with organizational systems and communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establishing and manager cytographic keys for cryotography employed in organizational dystems and communications sessions at the end of the sessio			
3.12.2 Develop and Implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in cognizational 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.28 3.13.5 SYSTEM AND COMMUNICATIONS PROTECTION 3.13.14 Monitor, control, and protect communications (e.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries or operational 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 Separate user functionality from system management functionality. 3.13.5 Separate user functionality from system management functionality. 3.13.6 Prevent unauthorized and unintended information transfer system organizational systems. 3.13.5 Implements ubnetworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.6 Desymptoms of the property of the communications traffic by default and allow network communications traffic by cocyclon ties. device of communications traffic by all permit by exceptions. 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections or some development organizational systems and communications social systems organizational systems and communications associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cytography when used to protect the confidentiality of CUI. 4.13.13.10 Establish and manage cytography with a time of management of th			
Include or eliminate vulnerabilities in organizational systems. 13.123 Monitor socurity controls on an engoing basis to ensure the continued effectiveness of the controls. 23.142 Develop, Gournent, 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. 28 23.13.15 SYSTEM AND COMMUNICATIONS PROTECTION 23.13.15 Monitor, control, and protect communications (e.e., information transmitted or received by organizational systems) at the externils obundaries and key internal boundaries of organizational systems and internal control of the system of the stemplant of the system of the stemplant of the stemplan	• • • • • • • • • • • • • • • • • • • •		
3.12.4 Develop, document, and periodically update system security plans that deservine so of the continued effect whereas of the continued and uniformation of programments are implemented, and the relationships with or connections to other systems. 3.13.5 PISTEM AND COMMUNICATIONS PROTECTION 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 security within organizational systems. 3.13.3 Spariate user functionality from system management functionality. 3.13.4 Prevent unauthorized and unintended information transfer via shared system resources. 3.13.5 Implement subneworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.6 Deep network communications traffic by default and allow network communications traffic by allowing and the reception. 3.13.1 Pimilate network communications traffic by default and allow network communications traffic by allowing mon-remote connections of organizational systems. 3.13.2 Implement cryptographic mechanisms to prevent unauthorized disclosure of CII during transmission unless otherwise protected by alternative physical safe, and the medical properties of the communications of collaborative computing devices and provide indication of devices from simultaneously establishing non-remote connection to associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.1 Employer provides the connection of collaborative computing devices and provide indication of devices in use to users prevent at the device.29 3.13.1 Ferrolate and monitor the use of robli	, , ,		
tiveness of the controls. 3.124 Develop, obcument, 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. 28 3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems). 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. 3.13.2 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 Separate user functionality from system management functionality. 3.13.5 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems in subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.6 Emplement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.6 Emplement subnetworks for simultaneously establishing non-remote connections with organizational systems and communications traffic by alpermit by exception. 3.13.8 Emplement cryptographic enclassins to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. 3.13.8 Implement cryptographic enclassins to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. 3.13.8 Implement subnervis (i.e., split tunnelling). 3.13.8 Implement cryptographic expensions of the enclassins to prevent in a defined period of inactivity. 3.13.8 Implement subnervis (i.e.,	ž ,		
3.13.2 Prevent unarthorized and unintended information security within organizational systems. 3.13.3 Systems and communications (i.e., information transmitted or received by organizational systems). 3.13.4 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 unarthorized and unintended information transfer via shared system resources. 3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.5 Prevent unarthorized and unintended information transfer via shared system resources. 3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.5 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connections with organizational systems and communicating via some other connections with organizational systems and communicating via some other connections of the sessions or after a defined protected by alternative physical safe-gourds. 3.13.6 Protect the confidentially of Cul. a rest. 3.13.11 Exploital and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3.13.12 Provibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. 29 3.13.13 Frotect the confidentially of Cul at rest. 3.14.1 Mentily proport, and correct system flaws in simely manner. 3.14.2 Provide protection from malicious code or devices and advisories and take action in response. 3.14.3 Provide pro	,		
scribe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.28 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 of 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 Fiverent unauthorized and unintended information transfer via shared system resources. 3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.6 Deep network communications traffic by default and allow network communications traffic by exception (i.e., days) all, permit by exception. 3.13.6 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). 3.13.8 Implement cryptographic remonshams to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. 3.13.9 Implement cryptographic keys for cryptography employed in organizational systems and communications associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.15 Protect the autheriticity of communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.16 Protect the autheriticity of communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.15 Protect the autheriticity of communications sessions at the end of the			
ments are implemented, and the relationships with or connections to other systems.28 3.13 SYSTEM AND COMMUNICATIONS PROTECTION 3.13 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. 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within 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 Esparate user functionality from system management functionality. 3.13.4 Prevent unuthorized and unintended information transfer via shared system resources. 3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.6 Deny network communications straffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). 3.13.6 Prevent remote devices from internal networks. 3.13.6 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safe-squards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.19 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.19 Terminate network connections associated with communications or provide indication of devices in use to users present at the device. 29 3.13.11 Employ P			
1.3.5 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 physically or logically separated from internal networks. 3.13.5 Deary network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external network (i.e., plit runningly). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safe-guards. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Establish and manage cryptography when used to protect the confidentiality of CUI. 3.13.12 Frohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of mobile code. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.13.16 Protect the confidentiality of CUI at rest. 3.13.17 System AND INFORMATION INTERITY 4.14 Lights mallicious code protection mechanisms when new releases are available.			
3.13 STEM AND COMMUNICATIONS PROTECTION 3.13 Montro, 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 the external 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. 3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. 3.13.3 Experience user functionality from system management functionality, 3.13.4 Prevent unauthorized and unintended information transfer via shared system resources. 3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.6 Derny rework communications straffic by default and allow network communications traffic by exception (i.e., dery all, permit by exception). 3.13.6 Prevent meda devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communications sessions of the connections in such as a defined period of inactivity. 3.13.9 Freminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Experience the extention of collaborative computing devices and provide indication of devices in use to users present at the device. 29 3.13.13 Fortical and monitor the use of mobile code. 3.13.14 Control and monitor the use of viole over internet Protocol (VoIP) technologies. 3.13.15 Protect the confidentiality of CUI at rest. 3.14.1 Specific			
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 physically or logically separated from internal networks. 3.13.6 Dery network communications traffic by default and allow network communications traffic by exception (i.e., deep val, permit by exception). 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external network (i.e., pilt tunneling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of Cull during transmission unless otherwise protected by alternative physical safe-guards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Englash and manage cryptographic when used to protect the confidentiality of Cul. 3.13.12 Protect the authenticity of communications sessions. 3.13.13 Protect the authenticity of communications sessions. 3.13.14 Control and monitor the use of Morcie over Internet Protocol (VoiP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of Cul at rest. 3.14.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of Cul at rest. 3.14.16 Protect the confidentiality			
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 security within organizational systems. 3.13.3 Separate user functionality from system management functionality. 3.13.4 Prevent nauthorized and unintended information transfer via shared system resources. 3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.6 Deep network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). 3.13.6 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safe-guards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employs PliS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. 3.13.14 Control and monitor the use of Wolke over Internet Protocol (VoIP) technologies. 3.13.15 Protoct the authenticity of communications sessions. 3.13.16 Protoct the confidentiality of CUI at rest. 3.14.16 System AND INFORMATION INTEGRITY 3.14.16 System AND INFORMATION INTEGRITY 3.14.16 Intentity, report, and correct system flaws in a timely manner. 3.14.17 System Shall NIFFORMATION INTEGRITY in the action in response. 3.14.16 Pr			
boundaries of organizational systems. 1.13.2 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 physically or logically separated from internal networks. 3.13.6 Derny network communications traffic by default and allow network communications traffic by exception (i.e., dept all, permit by exception). 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). 3.13.8 Implement cryptographic well-anisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 English and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 English and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 English and manage cryptographic keys for cryptographic keys or c			
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 physically or logically separated from internal networks. 3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connections or starting the systems and communicating via some other connections or starting the systems and communicating via some other connections or starting the systems and communicating via some other connections or starting via some other connection to resources in external networks (i.e., split tunneling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safe-guards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period inactivity. 3.13.10 Establish and manage cryptography when used to protect the confidentiality of CUI. 3.13.11 Employ FiPS-validated cryptography when used to protect the confidentiality of Cuir sets. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of Molice doe. 4 Y Currently we have no mobile code 3.13.14 Control and monitor the use of mobile code. 4 Y Currently we have no mobile code 5.13.14 Systems AND INFORMATION INTEGRITY 5.14.14 United a malicious code protection from malicious code at designated locations wi			
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 physically or logically separated from internal networks. 3.13.6 Derry network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunnelling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safe-guards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.11 Employ FIPS-validated cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14.16 Protect the confidentiality of CUI at rest. 3.14.18 SYSTEM AND INFORMATION INTEGRITY 3.14.18 Gentry system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection from malicious code at designated locations within organizational systems.	<u> </u>		
tional systems. 3.13.3 Separate user functionality from system management functionality. 3.13.4 Prevent unauthorized and unintended information transfer via shared system resources. 3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device 29 and indication of devices in use to users present at the device 29 and indication of devices in use to users present at the device 29 and indication of devices in use to users present at the device 29 and indication of devices in use to users present at the device 29 and indication of devices in use to users present at the device 29 and indication of devices in use to users present at the device 29 and indication of devices in use to users present at the device 29 and indication of devices in use to users present at the device 29 and indication of devices in use to users present at the device 29 and indication of devices in use to users present at the device 29 and indication of devices in use to users present at the device 29 and in a device in use to users present at the device 29 and in a de			
3.13.3 Separate user functionality from system management functionality. 3.13.4 Prevent unauthorized and unintended information transfer via shared system resources. 3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., spilt tunneling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safe-guards. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of Mobile code. 3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.14.11 Identify, report, and correct system flaws in a timely manner. 3.14.13 Intensity report, and correct system flaws in a timely manner. 3.14.14 Prohibit remote activation of advisories and take action in response. 3.14.14 Update malicious code protection from malicious code at designated locations within organizational systems. 3.14.14 Prohibit reports and correct system flaws in a timely manner. 3.14.14 Prohibit reports and control mechanisms when new releases are available.			
3.13.1 Prevent unauthorized and unintended information transfer via shared system resources. 3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safe-guards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of Voice over internet Protocol (VoIP) technologies. 3.13.14 Control and monitor the use of Voice over internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Provide protection from malicious code at designated locations within organizational systems. 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Indentify report, and correct system flaws in a timely manner. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available.	-		
resources. 3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 3.13.6 Dery network communications traffic by default and allow network communications traffic by exception (i.g., deny all, permit by exception). 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of mobile code. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the uniformality of CUI at rest. 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y			
physically or logically separated from internal networks. 3.13.6 Dery network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.13 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of Mobile code. 3.13.14 Control and monitor the use of Mobile code. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14.1 Very protect of confidentiality of CUI at rest. 3.14.1 Provide protection from malicious code at designated locations within organizational systems. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files 4 Y			
physically or logically separated from internal networks. 3.13.6 Dery network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.13 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of Mobile code. 3.13.14 Control and monitor the use of Mobile code. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14.1 Very protect the confidentiality of CUI at rest. 3.14.1 Provide protection from malicious code at designated locations within organizational systems. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files 4 Y	3.13.5 Implement subnetworks for publicly accessible system components that are		
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safe-guards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of mobile code. 3.13.15 Protect the authenticity of communications sessions. 3.13.13 Frotect the authenticity of communications sessions. 3.13.14 Identify, report, and correct system flaws in a timely manner. 3.14.1 Venture proportion from malicious code at designated locations within organizational systems. 3.14.2 Provide protection from malicious code at designated locations within organizational systems.			
cations traffic by exception (i.e., deny all, permit by exception). 3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device 29 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of woice over internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14 System AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files 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 CUI during transmission unless otherwise protected by alternative physical safe-guards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of woice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the authenticity of communications sessions. 3.14.1 SySTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y			
resources in external networks (i.e., split tunneling). 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safe-guards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of Moice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y	3.13.7 Prevent remote devices from simultaneously establishing non-remote connec-		
3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safe-guards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of voice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the authenticity of communications sessions. 3.14.15 SYSTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y	tions with organizational systems and communicating via some other connection to		
CUI during transmission unless otherwise protected by alternative physical safeguards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of Mobile code. 3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y	resources in external networks (i.e., split tunneling).		
guards. 3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14.11 Identify, report, and correct system flaws in a timely manner. 3.14.12 Provide protection from malicious code at designated locations within organizational systems. 3.14.2 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files	3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of		
3,13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 3,13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3,13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3,13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3,13.13 Control and monitor the use of mobile code. 3,13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3,13.15 Protect the authenticity of communications sessions. 3,14.16 Protect the confidentiality of CUI at rest. 3,14.4 SYSTEM AND INFORMATION INTEGRITY 3,14.1 Identify, report, and correct system flaws in a timely manner. 3,14.2 Provide protection from malicious code at designated locations within organizational systems. 3,14.4 Update malicious code protection mechanisms when new releases are available. 3,14.5 Perform periodic scans of organizational systems and real-time scans of files Y	CUI during transmission unless otherwise protected by alternative physical safe-		
the end of the sessions or after a defined period of inactivity. 3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14.14 System AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y	guards.		
3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y	3.13.9 Terminate network connections associated with communications sessions at		
ganizational systems. 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14.18 Protect the confidentiality of CUI at rest. 3.14.19 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y	the end of the sessions or after a defined period of inactivity.		
3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y	3.13.10 Establish and manage cryptographic keys for cryptography employed in or-		
of CUI. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available.			
3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y	3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality		
indication of devices in use to users present at the device.29 3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files	of CUI.		
3.13.13 Control and monitor the use of mobile code. 3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files			
3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files	indication of devices in use to users present at the device.29		
gies. 3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y		Υ	Currently we have no mobile code
3.13.15 Protect the authenticity of communications sessions. 3.13.16 Protect the confidentiality of CUI at rest. 3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files	` '		
3.13.16 Protect the confidentiality of CUI at rest. 3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files	<u> </u>		
3.14 SYSTEM AND INFORMATION INTEGRITY 3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y	-		
3.14.1 Identify, report, and correct system flaws in a timely manner. 3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files	,		
3.14.2 Provide protection from malicious code at designated locations within organizational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files			
zational systems. 3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y			
3.14.3 Monitor system security alerts and advisories and take action in response. 3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y	i s		
3.14.4 Update malicious code protection mechanisms when new releases are available. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y	-		
able. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files Y			
3.14.5 Perform periodic scans of organizational systems and real-time scans of files		Y	
nom external sources as mes are downloaded, opened, or executed.		Y	
	nom external sources as mes are downloaded, opened, or executed.		



3.14.6 Monitor organizational systems, including inbound and outbound communi-	Y		
cations traffic, to detect attacks and indicators of potential attacks.			
Total requirements	109	9	
Total Rubin lintends to comply with	26	5	
Total Rubin Complies with in 2021	17	,	

B References

[NIST.FIPS.200], Division, C.S., 2006, Publication 200, minimum security requirements for federal information and information systems, URL https://doi.org/10.6028/NIST.FIPS.200

[NIST.SP.800-171], ROSS, R., VISCUSO, P., GUISSANIE, G., DEMPSEY, K., RIDDLE, M., 2020, Special publication 800-171, protecting controlled unclassified information in nonfederal systems and organizations, URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

C Acronyms

Description
Advanced Encryption Standard
Controlled Unclassified Information
Data Management
DM Technical Note
Department of Energy
Internet Protocol
National Institute of Standards and Technology (USA)
National Science Foundation
SLAC National Accelerator Laboratory
virtual private network
degree; unit of angle