DFARS Compliance Overview

CONFIDENTIAL This document and the information set forth herein are the proprietary property of Egnyte, and are to be held in confidence. No part of this document may be copied, reproduced or disclosed to third parties without the expressed written consent of Egnyte.	**Document Version:** 1.0
	Origination Date: 12/31/2017
	Revision Date: 01/12/2017
	Author: Kris Lahiri
	Status: Approved

Introduction

Egnyte recognizes that some of our customers may be subject to the new DFARS Department of Defense (DoD) requirements that came into effect on 12/31/2017.

On October 21, 2016, the Department of Defense (DoD) issued its Final Rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) and imposing safeguarding and cyber incident reporting obligations on defense contractors whose information systems process, store, or transmit covered defense information (CDI).
The final DFARS clause 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) specifies safeguards to include cyber incident reporting requirements and additional considerations for cloud service providers.

The DFARS clause 252.204-7012 leverages the NIST 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" standard, for the implementation of the associated controls required by the regulation.

Egnyte Solutions

Egnyte Connect is designed with business in mind, so IT can focus on security & performance, while users can access all their content from their desktop, mobile and browser.

Egnyte Protect is the industry's first cloud-based content governance solution. It provides you with powerful and easy-to-use tools to protect your employee and customer privacy, intellectual property, and confidential information. Egnyte Protect finds where your sensitive content is and centrally enforces your access policies across content repositories to maximize control and security.

DFARS Compliance

Egnyte currently does not deal directly with DoD customers, however has been requested by several customers to be DFARS compliant. Although DFARS does not directly regulate Egnyte, Egnyte is considered within the supply chain or "flow down" from customers who do have DoD customers.

Egnyte will not directly receive Controlled Unclassified Information (CUI). Any CUI placed within the Egnyte platform is not accessible due to the transmission and storage encryption mechanisms Egnyte has in place on all production systems.

With that said, Egnyte has drafted this overview to provide our customers with a mapping based on NIST 800-171 Appendix D tables containing the 109 control requirements and has mapped our policies, procedures and controls that are in place under the ISO27001 and ISO27018 certifications.

These mappings provide assurance to our customers impacted by DFARS that Egnyte has the necessary controls in place to meet the NIST 800-171 control requirements through the implementation of the ISO27001 controls. Egnyte does not exclude any ISO27001 or ISO27018 controls under the certification and has been in place since 2015.

Egnyte is currently also undergoing SSAE18 SOC 2 Type 2 attestation in 2018 utilizing many of the same controls that would be leveraged for NIST 800-171.

NIST 800-171 Standards - Egnyte Process Area Mapping

The table below is derived from Appendix D within the NIST 800-171 standard available here: https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

NIST 800-171, with the applicable Egnyte process area mapped to the controls.
NIST 800-171 leverages NIST 800-53 Moderate controls for its implemented requirements.

NIST 800-171 Control Number	Control Family	Control Text	Egnyte Process Mapping	NIST 800-53 Mapping	ISO 27002:2013 Mapping
3.1.1	Access Control	Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).	Access Control Policy and Procedure	AC-2, AC-3, AC-17	A.6.2.1, A.6.2.2, A.6.2.2, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.13.1.1, A.13.2.1, A.14.1.2, A.14.1.2, A.14.1.3, A.18.1.3
3.1.2	Access Control	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Access Control Policy and Procedure	AC-2, AC-3, AC-17	A.6.2.1, A.6.2.2, A.6.2.2, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.13.1.1, A.13.2.1, A.14.1.2, A.14.1.2, A.14.1.3, A.18.1.3
3.1.3	Access Control	Control the flow of CUI in accordance with approved authorizations.	Access Control Policy and Procedure	AC-4	A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3

3.1.4	Access Control	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Access Control Policy and Procedure	AC-5	A.6.1.2
3.1.5	Access Control	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Access Control Policy and Procedure	AC-6, AC-6(1), AC-6(5)	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5
3.1.6	Access Control	Use non-privileged accounts or roles when accessing nonsecurity functions.	Access Control Policy and Procedure	AC-6(2)	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5
3.1.7	Access Control	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	Access Control Policy and Procedure	AC-6(9), AC-6(10)	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5
3.1.8	Access Control	Limit unsuccessful logon attempts.	Access Control Policy and Procedure	AC-7	A.9.4.2
3.1.9	Access Control	Provide privacy and security notices consistent with applicable CUI rules.	Access Control Policy and Procedure	AC-9	A.9.4.2
3.1.10	Access Control	Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.	Access Control Policy and Procedure	AC-11, AC-11(1)	A.11.2.8, A.11.2.9
3.1.11	Access Control	Terminate (automatically) a user session after a defined condition.	Access Control Policy and Procedure	AC-12	None
3.1.12	Access Control	Monitor and control remote access sessions.	Access Control Policy and Procedure	AC-17(1)	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
3.1.13	Access Control	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Access Control Policy and Procedure	AC-17(2)	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
3.1.14	Access Control	Route remote access via managed access control points.	Access Control Policy and Procedure	AC-17(3)	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
3.1.15	Access Control	Authorize remote execution of privileged commands and remote access to security-relevant information.	Access Control Policy and Procedure	AC-17(4)	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
3.1.16	Access Control	Authorize wireless access prior to allowing such connections.	Access Control Policy and Procedure	AC-18	A.6.2.1, A.13.1.1, A.13.2.1
3.1.17	Access Control	Protect wireless access using authentication and encryption.	Access Control Policy and Procedure	AC-18(1)	A.6.2.1, A.13.1.1, A.13.2.1
3.1.18	Access Control	Control connection of mobile devices.	Mobile Device Policy and Procedure	AC-19	A.6.2.1, A.11.2.6, A.13.2.1

3.1.19	Access Control	Encrypt CUI on mobile devices and mobile computing platforms.	Mobile Device Policy and Procedure	AC-19(5)	A.6.2.1, A.11.2.6, A.13.2.1
3.1.20	Access Control	Verify and control/limit connections to and use of external systems.	Access Control Policy and Procedure	AC-20, AC-20(1)	A.11.2.6, A.13.1.1, A.13.2.1
3.1.21	Access Control	Limit use of organizational portable storage devices on external systems.	Access Control Policy and Procedure	AC-20(2)	A.11.2.6, A.13.1.1, A.13.2.1
3.1.22	Access Control	Control CUI posted or processed on publicly accessible systems.	Access Control Policy and Procedure	AC-22	None
3.2.1	Awareness and Training	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.	Awareness and Training	AT-2, AT-3	A.7.2.2, A.12.2.1
3.2.2	Awareness and Training	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	Awareness and Training	AT-2, AT-3	A.7.2.2, A.12.2.1
3.2.3	Awareness and Training	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Awareness and Training	AT-2(2)	A.7.2.2, A.12.2.1
3.3.1	Audit and Accountability	Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	Audit and Accountability	AU-2, AU-3, AU-3(1), AU-6, AU-12	A.12.4.1, A.12.4.3, A.16.1.2, A.16.1.4
3.3.2	Audit and Accountability	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	Audit and Accountability	AU-2, AU-3, AU-3(1), AU-6, AU-12	A.12.4.1, A.12.4.3, A.16.1.2, A.16.1.4
3.3.3	Audit and Accountability	Review and update audited events.	Audit and Accountability	AU-2(3)	None
3.3.4	Audit and Accountability	Alert in the event of an audit process failure.	Audit and Accountability	AU-5	None
3.3.5	Audit and Accountability	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	Audit and Accountability	AU-6(1), AU-6(3)	A.12.4.1, A.16.1.2, A.16.1.4
3.3.6	Audit and Accountability	Provide audit reduction and report generation to support on-demand analysis and reporting.	Audit and Accountability	AU-7	None
3.3.7	Audit and Accountability	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	Audit and Accountability	AU-8, AU-8(1)	A.12.4.4

3.3.8	Audit and Accountability	Protect audit information and audit tools from unauthorized access, modification, and deletion.	Audit and Accountability	AU-9	A.12.4.2, A.12.4.3, A.18.1.3
3.3.9	Audit and Accountability	Limit management of audit functionality to a subset of privileged users.	Audit and Accountability	AU-9(4)	A.12.4.2, A.12.4.3, A.18.1.3
3.4.1	Configuration Management	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Configuration Management Policy and Procedure	CM-2, CM-6, CM-8, CM-8(1)	A.8.1.1, A.8.1.2
3.4.2	Configuration Management	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Configuration Management Policy and Procedure	CM-2, CM-6, CM-8, CM-8(1)	A.8.1.1, A.8.1.2
3.4.3	Configuration Management	Track, review, approve/disapprove, and audit changes to organizational systems.	Configuration Management Policy and Procedure	CM-3	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
3.4.4	Configuration Management	Analyze the security impact of changes prior to implementation.	Configuration Management Policy and Procedure	CM-4	A.14.2.3
3.4.5	Configuration Management	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	Configuration Management Policy and Procedure	CM-5	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1
3.4.6	Configuration Management	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Configuration Management Policy and Procedure	CM-7	A.12.5.1 (ISO control doesn't completely match NIST 800-53)
3.4.7	Configuration Management	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	Configuration Management Policy and Procedure	CM-7(1), CM-7(2)	A.12.5.1 (ISO control doesn't completely match NIST 800-53)
3.4.8	Configuration Management	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	Configuration Management Policy and Procedure	CM-7(4), CM-7(5)	A.12.5.1 (ISO control doesn't completely match NIST 800-53)
3.4.9	Configuration Management	Control and monitor user-installed software.	Configuration Management Policy and Procedure	CM-11	A.12.5.1, A.12.6.2
3.5.1	Identification and Authentication	Identify system users, processes acting on behalf of users, or devices.	Access Control Policy and Procedure	IA-2, IA-5	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3

3.5.2	Identification and Authentication	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.	Access Control Policy and Procedure	IA-2, IA-5	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3
3.5.3	Identification and Authentication	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Access Control Policy and Procedure	IA-2(1), IA-2(2), IA-2(3)	A.9.2.1
3.5.4	Identification and Authentication	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	Access Control Policy and Procedure	IA-2(8), IA-2(9)	A.9.2.1
3.5.5	Identification and Authentication	Prevent reuse of identifiers for a defined period.	Access Control Policy and Procedure	IA-4	A.9.2.1
3.5.6	Identification and Authentication	Disable identifiers after a defined period of inactivity.	Access Control Policy and Procedure	IA-4	A.9.2.1
3.5.7	Identification and Authentication	Enforce a minimum password complexity and change of characters when new passwords are created.	Password Policy and Procedure	IA-5(1)	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3
3.5.8	Identification and Authentication	Prohibit password reuse for a specified number of generations.	Password Policy and Procedure	IA-5(1)	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3
3.5.9	Identification and Authentication	Allow temporary password use for system logons with an immediate change to a permanent password.	Password Policy and Procedure	IA-5(1)	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3
3.5.10	Identification and Authentication	Store and transmit only cryptographically-protected passwords.	Password Policy and Procedure	IA-5(1)	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3
3.5.11	Identification and Authentication	Obscure feedback of authentication information.	Password Policy and Procedure	IA-5(1)	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3
3.6.1	Incident Response	Establish an operational incident-handling capability for organizational systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.	Incident Management Policy and Procedure	IR-2, IR-4, IR-5, IR-6, IR-7	A.6.1.3, A.7.2.2 (ISO Control doesn't completely match NIST 800-53), A.16.1.2, A.16.1.4, A.16.1.5, A.16.1.6
3.6.2	Incident Response	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.	Incident Management Policy and Procedure	IR-2, IR-4, IR-5, IR-6, IR-7	A.6.1.3, A.7.2.2 (ISO Control doesn't completely match NIST 800-53), A.16.1.2, A.16.1.4,

					A.16.1.5, A.16.1.6
3.6.3	Incident Response	Test the organizational incident response capability.	Incident Management Policy and Procedure	IR-3, IR-3(2)	None
3.7.1	Maintenance	Perform maintenance on organizational systems.	Asset Management Policy and Procedure	MA-2, MA-3, MA-3(1), MA-3(2)	A.11.2.4, A.11.2.5 (ISO Controls don't completely match NIST 800-53)
3.7.2	Maintenance	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	Asset Management Policy and Procedure	MA-2, MA-3, MA-3(1), MA-3(2)	A.11.2.4, A.11.2.5 (ISO Controls don't completely match NIST 800-53)
3.7.3	Maintenance	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Asset Management Policy and Procedure	MA-2	A.11.2.4, A.11.2.5 (ISO Controls don't completely match NIST 800-53)
3.7.4	Maintenance	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	Asset Management Policy and Procedure	MA-3(2)	None
3.7.5	Maintenance	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Asset Management Policy and Procedure	MA-4	None
3.7.6	Maintenance	Supervise the maintenance activities of maintenance personnel without required access authorization.	Asset Management Policy and Procedure	MA-5	None
3.8.1	Media Protection	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	Data Classification Policy and Procedure Asset Management Policy and Procedure	MP-2, MP-4, MP-6	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.11.2.9
3.8.2	Media Protection	Limit access to CUI on system media to authorized users.	Data Classification Policy and Procedure Asset Management Policy and Procedure	MP-2, MP-4, MP-6	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.11.2.9

3.8.3	Media Protection	Sanitize or destroy system media containing CUI before disposal or release for reuse.	Data Classification Policy and Procedure Asset Management Policy and Procedure	MP-2, MP-4, MP-6	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.11.2.9
3.8.4	Media Protection	Mark media with necessary CUI markings and distribution limitations.	Data Classification Policy and Procedure Asset Management Policy and Procedure	MP-3	A.8.2.2
3.8.5	Media Protection	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	Data Classification Policy and Procedure Asset Management Policy and Procedure	MP-5	A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.5, A.11.2.6
3.8.6	Media Protection	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	Data Classification Policy and Procedure Asset Management Policy and Procedure	MP-5(4)	A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.5, A.11.2.6
3.8.7	Media Protection	Control the use of removable media on system components.	Data Classification Policy and Procedure Asset Management Policy and Procedure	MP-7	A.8.2.3, A.8.3.1
3.8.8	Media Protection	Prohibit the use of portable storage devices when such devices have no identifiable owner.	Data Classification Policy and Procedure Asset Management Policy and Procedure	MP-7(1)	A.8.2.3, A.8.3.1
3.8.9	Media Protection	Protect the confidentiality of backup CUI at storage locations.	Backup Policy and Procedure	CP-9	A.12.3.1, A.17.1.2, A.18.1.3
3.9.1	Personnel Security	Screen individuals prior to authorizing access to organizational systems containing CUI.	Human Resources Policy and Procedure	PS-3, PS-4, PS-5	A.7.1.1, A.7.3.1, A.8.1.4
3.9.2	Personnel Security	Ensure that CUI and organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Human Resources Policy and Procedure	PS-3, PS-4, PS-5	A.7.1.1, A.7.3.1, A.8.1.4
3.10.1	Physical Protection	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	Physical & Environmental Security Policy and Procedure	PE-2, PE-5, PE-6	A.11.1.2, A.11.1.3

3.10.2	Physical Protection	Protect and monitor the physical facility and support infrastructure for organizational systems.	Physical & Environmental Security Policy and Procedure	PE-2, PE-5, PE-6	A.11.1.2, A.11.1.3
3.10.3	Physical Protection	Escort visitors and monitor visitor activity.	Physical & Environmental Security Policy and Procedure	PE-3	A.11.1.1, A.11.1.2, A.11.1.3
3.10.4	Physical Protection	Maintain audit logs of physical access.	Physical & Environmental Security Policy and Procedure	PE-3	A.11.1.1, A.11.1.2, A.11.1.3
3.10.5	Physical Protection	Control and manage physical access devices.	Physical & Environmental Security Policy and Procedure	PE-3	A.11.1.1, A.11.1.2, A.11.1.3
3.10.6	Physical Protection	Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).	BCP DR Policy and Procedure Remote Access Policy and Procedure	PE-17	A.6.2.2, A.11.2.6, A.13.2.1
3.11.1	Risk Assessment	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	Information Security Governance Policy and Procedure	RA-3	A.12.6.1 (ISO control doesn't completely match NIST 800-53)
3.11.2	Risk Assessment	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Configuration Management Policy and Procedure	RA-5, RA-5(5)	A.12.6.1 (ISO control doesn't completely match NIST 800-53)
3.11.3	Risk Assessment	Remediate vulnerabilities in accordance with assessments of risk.	Configuration Management Policy and Procedure	RA-5	A.12.6.1 (ISO control doesn't completely match NIST 800-53)
3.12.1	Security Assessment	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Compliance Policy and Procedure	CA-2, CA-5, CA-7	A.14.2.8, A.18.2.2, A.18.2.3 (for CA-2 only)
3.12.2	Security Assessment	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Compliance Policy and Procedure	CA-2, CA-5, CA-7	A.14.2.8, A.18.2.2, A.18.2.3 (for CA-2 only)
3.12.3	Security Assessment	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Compliance Policy and Procedure	CA-2, CA-5, CA-7	A.14.2.8, A.18.2.2, A.18.2.3 (for CA-2 only)
3.12.4	Security Assessment	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are	Compliance Policy and Procedure		

		implemented, and the relationships with or connections to other systems.			
3.13.1	System and Communications Protection	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.	Infrastructure Security Policy and Procedure Production Access Policy and Procedure	SC-7, SA-8	A.8.2.3, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
3.13.2	System and Communications Protection	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	Infrastructure Security Policy and Procedure Production Access Policy and Procedure	SC-7, SA-8	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3, A.14.2.5
3.13.3	System and Communications Protection	Separate user functionality from system management functionality.	Infrastructure Security Policy and Procedure Production Access Policy and Procedure	SC-2	None
3.13.4	System and Communications Protection	Prevent unauthorized and unintended information transfer via shared system resources.	Infrastructure Security Policy and Procedure Production Access Policy and Procedure	SC-4	None
3.13.5	System and Communications Protection	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Infrastructure Security Policy and Procedure Production Access Policy and Procedure	SC-7, SA-8	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3, A.14.2.5
3.13.6	System and Communications Protection	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Infrastructure Security Policy and Procedure Production Access Policy and Procedure	SC-7(5)	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3
3.13.7	System and Communications Protection	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks.	Remote Access Policy and Procedure	SC-7(7)	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3
3.13.8	System and Communications Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Cryptographic & Key Management Policy and Procedure	SC-8, SC-8(1)	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
3.13.9	System and Communications Protection	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Access Control Policy and Procedure	SC-10	A.13.1.1

3.13.10	System and Communications Protection	Establish and manage cryptographic keys for cryptography employed in organizational systems;	Cryptographic & Key Management Policy and Procedure	SC-12	A.10.1.2
3.13.11	System and Communications Protection	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Cryptographic & Key Management Policy and Procedure	SC-13	A.10.1.1, A.14.1.2, A.14.1.3, A.18.1.5
3.13.12	System and Communications Protection	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Remote Access Policy and Procedure	SC-15	A.13.2.1 (ISO control doesn't completely match NIST 800-53)
3.13.13	System and Communications Protection	Control and monitor the use of mobile code.	Anti-Virus, Malware Policy and Procedure	SC-18	None
3.13.14	System and Communications Protection	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	Infrastructure Security Policy and Procedure	SC-19	None
3.13.15	System and Communications Protection	Protect the authenticity of communications sessions.	Cryptographic & Key Management Policy and Procedure	SC-23	None
3.13.16	System and Communications Protection	Protect the confidentiality of CUI at rest.	Cryptographic & Key Management Policy and Procedure	SC-28	A.8.2.3 (ISO control doesn't completely match NIST 800-53)
3.14.1	System and Information Integrity	Identify, report, and correct information and system flaws in a timely manner.	Incident Management Policy and Procedure	SI-2, SI-3, SI-5	A.6.1.4 (ISO control doesn't completely match NIST 800-53), A.12.2.1, A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
3.14.2	System and Information Integrity	Provide protection from malicious code at appropriate locations within organizational systems.	Anti-Virus, Malware Policy and Procedure	SI-2, SI-3, SI-5	A.6.1.4 (ISO control doesn't completely match NIST 800-53), A.12.2.1, A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
3.14.3	System and Information Integrity	Monitor system security alerts and advisories and take appropriate actions in response.	Monitoring and Logging Policy and Procedure	SI-2, SI-3, SI-5	A.6.1.4 (ISO control doesn't completely match NIST 800-53),

					A.12.2.1, A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
3.14.4	System and Information Integrity	Update malicious code protection mechanisms when new releases are available.	Anti-Virus, Malware Policy and Procedure	SI-3	A.12.2.1
3.14.5	System and Information Integrity	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	System and Information Integrity	SI-3	A.12.2.1
3.14.6	System and Information Integrity	Monitor organizational systems including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	System and Information Integrity	SI-4, SI-4(4)	None
3.14.7	System and Information Integrity	Identify unauthorized use of organizational systems.	System and Information Integrity	SI-4	None