System Security Plan Template

Information System Name

Version 1.0

November 2024

Instructions

This document is intended as a starting point for the IT System Security plan required by NIST 800-171 revision 3 (03.15.02)

Each section includes a blue box of text like this which describes what the section is looking for and how to complete it. Once you have provided the information, you can remove this blue text.

This document has Confidential markings on it as the information provided once complete is considered confidential and should not be shared outside the organization, but the template itself can be shared.

Approved By: _____ Approval Date: _____
Insert Approver Title

Approved By: _____ Approval Date: _____
Insert Approver Title

Approved By: _____ Approval Date: _____
Insert Approver Title

Table of Contents

1 Document Revision History

This is not the Template's revision history, but the System Security Plan's revision history

Version	Date	Author	Description

2 Executive Summary

Provide a brief summary of work being completed under the contract. Information to consider includes:

- *An explanation of research or work being conducted*
- *What types of data/information are being processed, stored and transmitted?*
- *An overview of outside organizations with which the contract is involved and how the organizations interact with each other. Examples of outside organizations might include:*
- *Field centers, clinical sites, clinical reading centers, and data collection centers*
- *Third party IT support vendors, etc.*
- *The roles and responsibilities of personnel as it relates to information collection, storage and sharing*

3 System Identification

*Identify the system name, type and owners. In the context of NIST 800-171, a **system** is a complete set of computers that support the function. For example, if you have a web service, the computer system that runs the web server and the computer system that runs the database is considered part of the same **system**.*

Within this section consider including:

- *Name of system(s)*
- *Whether it is a major application (ex. database/custom code) or general support system (ex. windows AD)*
- *System Information Type: Management and Support or Research focused*
- *A list of individuals who have administrative rights to workstations and servers*
- *Ownership contacts: Information Owner, Information Systems Owner*

Information System Owner – the system owner of functional proponent/advocate for this system *(usually the researcher)*	
Name	
Title	
Department	

Phone Number	
Email	

Information System Management *(any IT staff assisting in the management of the system)*	
Name	
Title	
Department	
Phone Number	
Email	

Copy and paste this table if more contacts are needed

4 System Operational Status

What is the current status of the system or parts of the system?
Operational – the system is in production
Under Development – the system is being designed, developed, or implemented
Undergoing a major modification – the system is undergoing a major conversion or transition

If the system is under development, outline the major activities and projected timeline to achieve operational status.

Operational

Any parts of your system that are already operational

Under Development

Any parts of the system that are still under development

Major Modification

Any parts of the system that are undergoing a major modification

5 General System Description

Provide a general description of the system. Outline what scope the system plays in conducting work for the overall contract. Detail the major functions of the information system and an overview of the system architecture including hardware and software components. For example, you could provide details on:

Significant use cases or user stories the system implements
Significant data or information inputs and outputs

Outline what types of data is collected and stored on the major system components and identify which business entity controls the data.

6 System Environment

Include a system architecture diagram portraying all major functions within the system. Provide a detailed description of each major function. For example, description could include:

- *Physical location*
- *Vendors for commercial software*
- *Groups/entities who have access to major functions*
- *Operating system*
- *Make and Model*
- *Licensed software for major functions*
- *Anti-Virus*
- *Firewalls*
- *DMZ*
- *Elements such as:*
  - *Web, Database and Application servers*
  - *E-mail services such as Microsoft Exchange Servers*
  - *Web-based applications and major application components such as web services or infrastructure products such as software frameworks*
  - *User Workstations and workstation software and specialized configurations*
  - *Scientific instruments and medical devices*
  - *Laboratory Information Systems*

Be sure to identify the organization that hosts and manages each major function.

System Threats

Outline the major threats to this system above and beyond any that are threats as a whole
e.g. This system processes CUI, so there is a threat from nation-state actors
e.g. This system is in a public space, so there is a threat to the physical security of the system

7 System Interconnections/Information Sharing

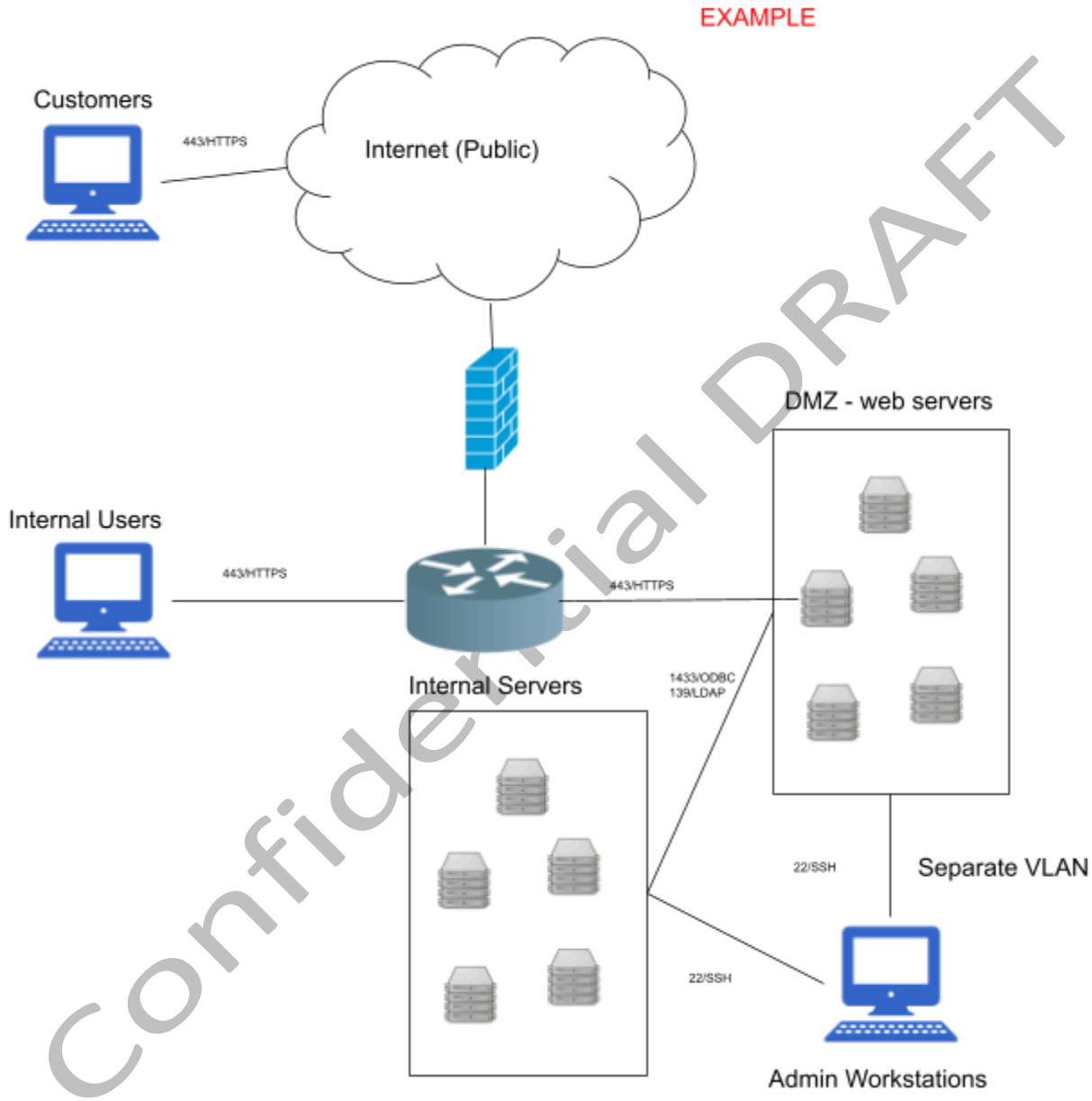
Outline the major connections to the system, how information is shared, stored and backed up, and what types of information is transmitted. For example, detail any connections that occur through public facing web-applications, internal intranet connections and remote connections to the system. Outline the security measures that are in place to protect information such as remote VPN, HTTPS and user agreements. This is a narrative of your data flow diagram. It should include

Table 2 - System Interconnections

IP Address and Interface	External Organization Name and IP Address of System	External Point of Contact and Phone Number	Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)	Data Direction (incoming, outgoing, or both)	Information Being Transmitted	Port Numbers
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>

Data Flow

Describe the flow of data in and out of system boundaries and insert a data flow diagram. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users. If necessary, include multiple data flow diagrams.



Ports, Protocols, and Services

These are the ports, protocols and services running on this system.

Table 2 - Ports, Protocols and Services

Ports (TCP/UDP)	Protocol(s)	Service(s)/App ID	Purpose	Used By
TCP/443	*HTTPS*	*IIS/web server*	*Allows access to public facing web server - informational*	*Public*
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>

What Ports, Protocols and Services are running on these systems? Include all open ports on all systems involved, indicate which ones are available to external systems. Indicate all major services running on all systems - ex. Active Directory, HTTPS, LDAP, ODBC, etc. Indicate all major protocols running - ex: HTTP and HTTPS, SSH, etc - these may be related to services. The first line is an example.

8 Enduring Exceptions

Are there any components of the system that have enduring exceptions? Enduring exceptions are where a security control cannot be met due to the nature of the component (ex. anti-malware on test equipment), or the system is configured in a particular way to match a contract (ex. equipment in the field, etc)

9 Minimum Security Controls

These are the minimum required security controls to meet NIST SP 800-171 revision 3.

When completing this section, be sure to address all of the assessment objectives listed for each control. Ideally, the description includes which assessment objective is met for each portion. Evidence and Documentation (Policies, Standards, Procedures, Guidance) should be at least linked from this SSP.

03.01 AC - Access Control

03.01.01 Account Management

03.01.01	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.01.01.ODP[01]**: *the time period for account inactivity before disabling is defined*. **A.03.01.01.ODP[02]**: *the time period within which to notify account managers and designated personnel or roles when accounts are no longer required is defined*. **A.03.01.01.ODP[03]**: *the time period within which to notify account managers and designated personnel or roles when users are terminated or transferred is defined*. **A.03.01.01.ODP[04]**: *the time period within which to notify account managers and designated personnel or roles when system usage or the need-to-know changes for an individual is defined*. **A.03.01.01.ODP[05]**: *the time period of expected inactivity requiring users to log out of the system is defined*. **A.03.01.01.ODP[06]**: *circumstances requiring users to log out of the system are defined*. **A.03.01.01.a[01]**: system account types allowed are defined. **A.03.01.01.a[02]**: system account types prohibited are defined. **A.03.01.01.b[01]**: system accounts are created in accordance with organizational policy, procedures, prerequisites, and criteria. **A.03.01.01.b[02]**: system accounts are enabled in accordance with organizational policy, procedures, prerequisites, and criteria. **A.03.01.01.b[03]**: system accounts are modified in accordance with organizational policy, procedures, prerequisites, and criteria. **A.03.01.01.b[04]**: system accounts are disabled in accordance with organizational policy, procedures, prerequisites, and criteria. **A.03.01.01.b[05]**: system accounts are removed in accordance with organizational policy, procedures, prerequisites, and criteria. **A.03.01.01.c.01**: authorized users of the system are specified. **A.03.01.01.c.02**: group and role memberships are specified. **A.03.01.01.c.03**: access authorizations (i.e., privileges) for each account are specified. **A.03.01.01.d.01**: access to the system is authorized based on a valid access authorization.	

A.03.01.01.d.02: access to the system is authorized based on intended system usage.

A.03.01.01.e: the use of system accounts is monitored.

A.03.01.01.f.01: system accounts are disabled when the accounts have expired.

A.03.01.01.f.02: system accounts are disabled when the accounts have been inactive for *<A.03.01.01.ODP[01]: time period>*.

A.03.01.01.f.03: system accounts are disabled when the accounts are no longer associated with a user or individual.

A.03.01.01.f.04: system accounts are disabled when the accounts violate organizational policy.

A.03.01.01.f.05: system accounts are disabled when significant risks associated with individuals are discovered.

A.03.01.01.g.01: account managers and designated personnel or roles are notified within *<A.03.01.01.ODP[02]: time period>* when accounts are no longer required.

A.03.01.01.g.02: account managers and designated personnel or roles are notified within *<A.03.01.01.ODP[03]: time period>* when users are terminated or transferred.

A.03.01.01.g.03: account managers and designated personnel or roles are notified within *<A.03.01.01.ODP[04]: time period>* when system usage or the need-to-know changes for an individual.

A.03.01.01.h: users are required to log out of the system after *<A.03.01.01.ODP[05]: time period>* of expected inactivity or when the following circumstances occur: *<A.03.01.01.ODP[06]: circumstances>*.

03.01.02 Access Enforcement

03.01.02	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.01.02[01]:** approved authorizations for logical access to CUI are enforced in accordance with applicable access control policies. **A.03.01.02[02]:** approved authorizations for logical access to system resources are enforced in accordance with applicable access control policies.	

03.01.03 Information Flow Enforcement

03.01.03	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.01.03[01]:** approved authorizations are enforced for controlling the flow of CUI within the system. **A.03.01.03[02]:** approved authorizations are enforced for controlling the flow of CUI between connected systems.	

03.01.04 Separation of Duties

03.01.04	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.01.04.a:** duties of individuals requiring separation are identified. **A.03.01.04.b:** system access authorizations to support separation of duties are defined.	

03.01.05 Least Privilege

03.01.05	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

03.01.05	Control Summary Information

☐ Not applicable

What is the solution and how is it implemented?

A.03.01.05.ODP[01]: *security functions for authorized access are defined.*

A.03.01.05.ODP[02]: *security-relevant information for authorized access is defined.*

A.03.01.05.ODP[03]: *the frequency at which to review the privileges assigned to roles or classes of users is defined.*

A.03.01.05.a: system access for users (or processes acting on behalf of users) is authorized only when necessary to accomplish assigned organizational tasks.

A.03.01.05.b[01]: access to ***<A.03.01.05.ODP[01]: security functions>*** is authorized.

A.03.01.05.b[02]: access to ***<A.03.01.05.ODP[02]: security-relevant information>*** is authorized.

A.03.01.05.c: the privileges assigned to roles or classes of users are reviewed ***<A.03.01.05.ODP[03]: frequency>*** to validate the need for such privileges.

A.03.01.05.d: privileges are reassigned or removed, as necessary.

03.01.06 Least Privilege - Privileged Accounts

03.01.06	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.01.06.ODP[01]: *personnel or roles to which privileged accounts on the system are to be restricted are defined.*

A.03.01.06.a: privileged accounts on the system are restricted to ***<A.03.01.06.ODP[01]: personnel or roles>***.

A.03.01.06.b: users (or roles) with privileged accounts are required to use non-privileged accounts when accessing non-security functions or non-security information.

03.01.07 Least Privilege - Privileged Functions

a. Prevent non-privileged users from executing privileged functions.
b. Log the execution of privileged functions.

03.01.07	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.01.07.a:** non-privileged users are prevented from executing privileged functions. **A.03.01.07.b:** the execution of privileged functions is logged.	

03.01.08 Unsuccessful Logon Attempts

03.01.08	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.01.08.ODP[01]:** *the number of consecutive invalid logon attempts by a user allowed during a time period is defined*. **A.03.01.08.ODP[02]:** *the time period to which the number of consecutive invalid logon attempts by a user is limited is defined*. **A.03.01.08.ODP[03]:** *one or more of the following PARAMETER VALUES are selected: {the account or node is locked automatically for <A.03.01.08.ODP[04]: time period>; the account or node is locked automatically until released by an administrator; the next logon prompt is delayed automatically; the system administrator is notified automatically; other action is taken automatically}.* **A.03.01.08.ODP[04]:** *the time period for an account or node to be locked is defined (if selected)*. **A.03.01.08.a:** a limit of ***<A.03.01.08.ODP[01]: number>*** consecutive invalid logon attempts by a user during ***<A.03.01.08.ODP[02]: time period>*** is enforced. **A.03.01.08.b:** ***<A.03.01.08.ODP[03]: SELECTED PARAMETER VALUES>*** when the maximum number of unsuccessful attempts is exceeded.	

03.01.08	Control Summary Information

03.01.09 System Use Notification

AC.L2-3.1.7	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.01.09:** a system use notification message with privacy and security notices consistent with applicable CUI rules is displayed before granting access to the system.	

03.01.10 Device Lock

03.01.10	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.01.10.ODP[01]:** *one or more of the following PARAMETER VALUES are selected: {a device lock is initiated after <A.03.01.10.ODP[02]: time period> of inactivity; the user is required to initiate a device lock before leaving the system unattended}*. **A.03.01.10.ODP[02]:** *the time period of inactivity after which a device lock is initiated is defined (if selected)*. **A.03.01.10.a:** access to the system is prevented by ***<A.03.01.10.ODP[01]: SELECTED PARAMETER VALUES>***.	

03.01.10	Control Summary Information

A.03.01.10.b: the device lock is retained until the user reestablishes access using established identification and authentication procedures.

A.03.01.10.c: information previously visible on the display is concealed via device lock with a publicly viewable image.

03.01.11 Session Termination

03.01.11	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.01.11.ODP[01]: *conditions or trigger events that require session disconnect are defined.*

A.03.01.11: a user session is terminated automatically after ***<A.03.01.11.ODP[01]: conditions or trigger events>***.

03.01.12 Remote Access

03.01.12	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.01.12.a[01]: types of allowable remote system access are defined.
A.03.01.12.a[02]: usage restrictions are established for each type of allowable remote system access.
A.03.01.12.a[03]: configuration requirements are established for each type of allowable remote

03.01.12	Control Summary Information
system access. **A.03.01.12.a[04]:** connection requirements are established for each type of allowable remote system access. **A.03.01.12.b:** each type of remote system access is authorized prior to establishing such connections. **A.03.01.12.c[01]:** remote access to the system is routed through authorized access control points. **A.03.01.12.c[02]:** remote access to the system is routed through managed access control points. **A.03.01.12.d[1]:** remote execution of privileged commands is authorized. **A.03.01.12.d[2]:** remote access to security-relevant information is authorized.	

03.01.16 Wireless Access

03.01.16	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.01.16.a[01]:** each type of wireless access to the system is defined. **A.03.01.16.a[02]:** usage restrictions are established for each type of wireless access to the system. **A.03.01.16.a[03]:** configuration requirements are established for each type of wireless access to the system. **A.03.01.16.a[04]:** connection requirements are established for each type of wireless access to the system. **A.03.01.16.b:** each type of wireless access to the system is authorized prior to establishing such connections. **A.03.01.16.c:** wireless networking capabilities not intended for use are disabled prior to issuance and deployment. **A.03.01.16.d[01]:** wireless access to the system is protected using authentication. **A.03.01.16.d[02]:** wireless access to the system is protected using encryption.	

03.01.18 Access Control for Mobile Devices

03.01.18	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.01.18.a[01]:** usage restrictions are established for mobile devices. **A.03.01.18.a[02]:** configuration requirements are established for mobile devices. **A.03.01.18.a[03]:** connection requirements are established for mobile devices. **A.03.01.18.b:** the connection of mobile devices to the system is authorized. **A.03.01.18.c:** full-device or container-based encryption is implemented to protect the confidentiality of CUI on mobile devices.	

03.01.20 Use of External Systems

03.01.20	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.01.20.ODP[01]:** *security requirements to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are defined*. **A.03.01.20.a: the** use of external systems is prohibited unless the systems are specifically authorized. **A.03.01.20.b:** the following security requirements to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are established: ***<A.03.01.20.ODP[01]: security requirements>***. **A.03.01.20.c.01:** authorized individuals are permitted to use external systems to access the organizational system or to process, store, or transmit CUI only after verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied.	

03.01.20	Control Summary Information
A.03.01.20.c.02: authorized individuals are permitted to use external systems to access the organizational system or to process, store, or transmit CUI only after retaining approved system connection or processing agreements with the organizational entity hosting the external systems. **A.03.01.20.d:** the use of organization-controlled portable storage devices by authorized individuals on external systems is restricted.	

03.01.22 Publicly Accessible Content

03.01.22	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.01.22.a:** authorized individuals are trained to ensure that publicly accessible information does not contain CUI. **A.03.01.22.b[01]:** the content on publicly accessible systems is reviewed for CUI. **A.03.01.22.b[02]:** CUI is removed from publicly accessible systems, if discovered.	

03.02 AT – Awareness and Training

03.02.01 Literacy Training and Awareness

03.02.01	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented	

03.02.01	Control Summary Information

☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.02.01.ODP[01]: *the frequency at which to provide security literacy training to system users after initial training is defined*.

A.03.02.01.ODP[02]: *events that require security literacy training for system users are defined.*

A.03.02.01.ODP[03]: *the frequency at which to update security literacy training content is defined.*

A.03.02.01.ODP[04]: *events that require security literacy training content updates are defined.*

A.03.02.01.a.01[01]: security literacy training is provided to system users as part of initial training for new users.

A.03.02.01.a.01[02]: security literacy training is provided to system users ***<A.03.02.01.ODP[01]: frequency>*** after initial training.

A.03.02.01.a.02: security literacy training is provided to system users when required by system changes or following ***<A.03.02.01.ODP[02]: events>***.

A.03.02.01.a.03[01]: security literacy training is provided to system users on recognizing indicators of insider threat.

A.03.02.01.a.03[02]: security literacy training is provided to system users on reporting indicators of insider threat.

A.03.02.01.a.03[03]: security literacy training is provided to system users on recognizing indicators of social engineering.

A.03.02.01.a.03[04]: security literacy training is provided to system users on reporting indicators of social engineering.

A.03.02.01.a.03[05]: security literacy training is provided to system users on recognizing indicators of social mining.

A.03.02.01.a.03[06]: security literacy training is provided to system users on reporting indicators of social mining.

A.03.02.01.b[01]: security literacy training content is updated ***<A.03.02.01.ODP[03]: frequency>***.

A.03.02.01.b[02]: security literacy training content is updated following ***<A.03.02.01.ODP[04]: events>***.

03.02.02 Role-Based Training

03.02.02	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.02.02.ODP[01]:** *the frequency at which to provide role-based security training to assigned personnel after initial training is defined*. **A.03.02.02.ODP[02]:** *events that require role-based security training are defined*. **A.03.02.02.ODP[03]:** *the frequency at which to update role-based security training content is defined*. **A.03.02.02.ODP[04]:** *events that require role-based security training content updates are defined*. **A.03.02.02.a.01[01]:** role-based security training is provided to organizational personnel before authorizing access to the system or CUI. **A.03.02.02.a.01[02]:** role-based security training is provided to organizational personnel before performing assigned duties. **A.03.02.02.a.01[03]:** role-based security training is provided to organizational personnel ***<A.03.02.02.ODP[01]: frequency>*** after initial training. **A.03.02.02.a.02:** role-based security training is provided to organizational personnel when required by system changes or following ***<A.03.02.02.ODP[02]: events>***. **A.03.02.02.b[01]:** role-based security training content is updated ***<A.03.02.02.ODP[03]: frequency>***. **A.03.02.02.b[02]:** role-based security training content is updated following ***<A.03.02.02.ODP[04]: events>***.	

03.03 AU - Audit and Accountability

03.03.01 Event Logging

03.03.01	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented	

03.03.01	Control Summary Information

☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.03.01.ODP[01]: *event types selected for logging within the system are defined*.

A.03.03.01.ODP[02]: *the frequency of event types selected for logging are reviewed and updated.*

A.03.03.01.a: the following event types are specified for logging within the system: ***<A.03.03.01.ODP[01]: event types>***.

A.03.03.01.b[01]: the event types selected for logging are reviewed ***<A.03.03.01.ODP[02]: frequency>***.

A.03.03.01.b[02]: the event types selected for logging are updated ***<A.03.03.01.ODP[02]: frequency>***.

03.03.02 Audit Record Content

03.03.02	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.03.02.a.01: audit records contain information that establishes what type of event occurred.

A.03.03.02.a.02: audit records contain information that establishes when the event occurred.

A.03.03.02.a.03: audit records contain information that establishes where the event occurred.

A.03.03.02.a.04: audit records contain information that establishes the source of the event.

A.03.03.02.a.05: audit records contain information that establishes the outcome of the event.

A.03.03.02.a.06: audit records contain information that establishes the identity of the individuals, subjects, objects, or entities associated with the event.

A.03.03.02.b: additional information for audit records is provided, as needed.

03.03.03 Audit Record Generation

03.03.03	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.03.03.a:** audit records for the selected event types and audit record content specified in 03.03.01 and 03.03.02 are generated. **A.03.03.03.b:** audit records are retained for a time period consistent with the records retention policy.	

03.03.04 Response to Audit Logging Process Failures

03.03.04	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.03.04.ODP[01]:** *the time period for organizational personnel or roles receiving audit logging process failure alerts is defined*. **A.03.03.04.ODP[02]:** *additional actions to be taken in the event of an audit logging process failure are defined*. **A.03.03.04.a:** organizational personnel or roles are alerted in the event of an audit logging process failure within ***<A.03.03.04.ODP[01]: time period>***. **A.03.03.04.b:** the following additional actions are taken: ***<A.03.03.04.ODP[02]: additional actions>***.	

03.03.05 Audit Record Review, Analysis, and Reporting

03.03.05	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.03.05.ODP[01]:** *the frequency at which system audit records are reviewed and analyzed is defined*. **A.03.03.05.a:** system audit records are reviewed and analyzed ***<A.03.03.05.ODP[01]: frequency>*** for indications and the potential impact of inappropriate or unusual activity. **A.03.03.05.b:** findings are reported to organizational personnel or roles. **A.03.03.05.c[01]:** audit records across different repositories are analyzed to gain organization-wide situational awareness. **A.03.03.05.c[02]:** audit records across different repositories are correlated to gain organization-wide situational awareness.	

03.03.06 Audit Record Reduction and Report Generation

03.03.06	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.03.06.a[01]:** an audit record reduction and report generation capability that supports audit record review is implemented. **A.03.03.06.a[02]:** an audit record reduction and report generation capability that supports audit record analysis is implemented. **A.03.03.06.a[03]:** an audit record reduction and report generation capability that supports audit record reporting requirements is implemented.	

03.03.06	Control Summary Information

A.03.03.06.a[04]: an audit record reduction and report generation capability that supports after-the-fact investigations of incidents is implemented.

A.03.03.06.b[01]: the original content of audit records is preserved.

A.03.03.06.b[02]: the original time ordering of audit records is preserved.

03.03.07 Time Stamps

03.03.07	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.03.07.ODP[01]: *granularity of time measurement for audit record time stamps is defined***.**

A.03.03.07.a: internal system clocks are used to generate time stamps for audit records.

A.03.03.07.b[01]: time stamps are recorded for audit records that meet ***<A.03.03.07.ODP[01]: granularity of time measurement>***.

A.03.03.07.b[02]: time stamps are recorded for audit records that use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or include the local time offset as part of the time stamp.

03.03.08 Protection of Audit Information

03.03.08	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

03.03.08	Control Summary Information

A.03.03.08.a[01]: audit information is protected from unauthorized access, modification, and deletion.

A.03.03.08.a[02]: audit logging tools are protected from unauthorized access, modification, and deletion.

A.03.03.08.b: access to management of audit logging functionality is authorized to only a subset of privileged users or roles.

03.04 CM - Configuration Management

03.04.01 Baseline Configuration

03.04.01	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.04.01.ODP[01]: *the frequency of baseline configuration review and update is defined***.**

A.03.04.01.a[01]: a current baseline configuration of the system is developed.

A.03.04.01.a[02]: a current baseline configuration of the system is maintained under configuration control.

A.03.04.01.b[01]: the baseline configuration of the system is reviewed ***<A.03.04.01.ODP[01]: frequency>***.

A.03.04.01.b[02]: the baseline configuration of the system is updated ***<A.03.04.01.ODP[01]: frequency>***.

A.03.04.01.b[03]: the baseline configuration of the system is reviewed when system components are installed or modified.

A.03.04.01.b[04]: the baseline configuration of the system is updated when system components are installed or modified.

03.04.02 Configuration Settings

03.04.02	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.04.02.ODP[01]:** *configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are defined*. **A.03.04.02.a[01]:** the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are established and documented: ***<A.03.04.02.ODP[01]: configuration settings>***. **A.03.04.02.a[02]:** the following configuration settings for the system are implemented: ***<A.03.04.02.ODP[01]: configuration settings>***. **A.03.04.02.b[01]:** any deviations from established configuration settings are identified and documented. **A.03.04.02.b[02]:** any deviations from established configuration settings are approved.	

03.04.03 Configuration Change Control

03.04.03	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.04.03.a:** the types of changes to the system that are configuration-controlled are defined. **A.03.04.03.b[01]:** proposed configuration-controlled changes to the system are reviewed with explicit consideration for security impacts. **A.03.04.03.b[02]:** proposed configuration-controlled changes to the system are approved or disapproved with explicit consideration for security impacts.	

03.04.03	Control Summary Information

A.03.04.03.c[01]: approved configuration-controlled changes to the system are implemented.

A.03.04.03.c[02]: approved configuration-controlled changes to the system are documented.

A.03.04.03.d[01]: activities associated with configuration-controlled changes to the system are monitored.

A.03.04.03.d[02]: activities associated with configuration-controlled changes to the system are reviewed.

03.04.04 Impact Analyses

03.04.04	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.04.04.a: changes to the system are analyzed to determine potential security impacts prior to change implementation.

A.03.04.04.b: the security requirements for the system continue to be satisfied after the system changes have been implemented.

03.04.05 Access Restrictions for Change

03.04.05	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

03.04.05	Control Summary Information

A.03.04.05[01]: physical access restrictions associated with changes to the system are defined and documented.

A.03.04.05[02]: physical access restrictions associated with changes to the system are approved.

A.03.04.05[03]: physical access restrictions associated with changes to the system are enforced.

A.03.04.05[04]: logical access restrictions associated with changes to the system are defined and documented.

A.03.04.05[05]: logical access restrictions associated with changes to the system are approved.

A.03.04.05[06]: logical access restrictions associated with changes to the system are enforced.

03.04.06 Least Functionality

03.04.06	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.04.06.ODP[01]: *functions to be prohibited or restricted are defined***.**

A.03.04.06.ODP[02]: *ports to be prohibited or restricted are defined*.

A.03.04.06.ODP[03]: *protocols to be prohibited or restricted are defined*.

A.03.04.06.ODP[04]: *connections to be prohibited or restricted are defined*.

A.03.04.06.ODP[05]: *services to be prohibited or restricted are defined***.**

A.03.04.06.ODP[06]: *the frequency at which to review the system to identify unnecessary or nonsecure functions, ports, protocols, connections, or services is defined*.

A.03.04.06.a: the system is configured to provide only mission-essential capabilities.

A.03.04.06.b[01]: the use of the following functions is prohibited or restricted: ***<A.03.04.06.ODP[01]: functions>***.

A.03.04.06.b[02]: the use of the following ports is prohibited or restricted: ***<A.03.04.06.ODP[02]: ports>***.

A.03.04.06.b[03]: the use of the following protocols is prohibited or restricted: ***<A.03.04.06.ODP[03]: protocols>***.

A.03.04.06.b[04]: the use of the following connections is prohibited or restricted: ***<A.03.04.06.ODP[04]: connections>***.

03.04.06	Control Summary Information

A.03.04.06.b[05]: the use of the following services is prohibited or restricted: ***<A.03.04.06.ODP[05]: services>***.

A.03.04.06.c: the system is reviewed ***<A.03.04.06.ODP[06]: frequency>*** to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.

A.03.04.06.d: unnecessary or nonsecure functions, ports, protocols, connections, and services are disabled or removed.

03.04.08 Authorized Software - Allow by Exception

03.04.08	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.04.08.ODP[01]: *the frequency at which to review and update the list of authorized software programs is defined***.**

A.03.04.08.a: software programs authorized to execute on the system are identified.

A.03.04.08.b: a deny-all, allow-by-exception policy for the execution of authorized software programs on the system is implemented.

A.03.04.08.c: the list of authorized software programs is reviewed and updated ***<A.03.04.08.ODP[01]: frequency>***.

03.04.10 System Component Inventory

03.04.10	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

03.04.10	Control Summary Information

What is the solution and how is it implemented?

A.03.04.10.ODP[01]: *the frequency at which to review and update the system component inventory is defined*.

A.03.04.10.a: an inventory of system components is developed and documented.

A.03.04.10.b[01]: the system component inventory is reviewed ***<A.03.04.10.ODP[01]: frequency>***.

A.03.04.10.b[02]: the system component inventory is updated ***<A.03.04.10.ODP[01]: frequency>***.

A.03.04.10.c[01]: the system component inventory is updated as part of component installations.

A.03.04.10.c[02]: the system component inventory is updated as part of component removals.

A.03.04.10.c[03]: the system component inventory is updated as part of system updates.

03.04.11 Information Location

03.04.11	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.04.11.a[01]: the location of CUI is identified and documented.

A.03.04.11.a[02]: the system components on which CUI is processed are identified and documented.

A.03.04.11.a[03]: the system components on which CUI is stored are identified and documented.

A.03.04.11.b[01]: changes to the system or system component location where CUI is processed are documented.

A.03.04.11.b[02]: changes to the system or system component location where CUI is stored are documented.

03.04.12 System and Component Configuration for High-Risk Areas

03.04.12	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.04.12.ODP[01]:** *configurations for systems or system components to be issued to individuals traveling to high-risk locations are defined*. **A.03.04.12.ODP[02]:** *security requirements to be applied to the system or system components when individuals return from travel are defined*. **A.03.04.12.a:** systems or system components with the following configurations are issued to individuals traveling to high-risk locations: ***<A.03.04.12.ODP[01]: configurations>***. **A.03.04.12.b:** the following security requirements are applied to the system or system components when the individuals return from travel: ***<A.03.04.12.ODP[02]: security requirements>***.	

03.05 IA - Identification and Authentication

03.05.01 User Identification, Authentication, and Re-Authentication

03.05.01	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

03.05.01	Control Summary Information
☐ Not applicable	
What is the solution and how is it implemented? **A.03.05.01.ODP[01]:** *circumstances or situations that require re-authentication are defined*. **A.03.05.01.a[01]:** system users are uniquely identified. **A.03.05.01.a[02]:** system users are authenticated. **A.03.05.01.a[03]:** processes acting on behalf of users are associated with uniquely identified and authenticated system users. **A.03.05.01.b:** users are reauthenticated when ***<A.03.05.01.ODP[01]: circumstances or situations>***.	

03.05.02 Device Identification and Authentication

03.05.02	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.05.02.ODP[01]:** *devices or types of devices to be uniquely identified and authenticated before establishing a connection are defined***.** **A.03.05.02[01]: *<A.03.05.02.ODP[01]: devices or types of devices>*** are uniquely identified before establishing a system connection. **A.03.05.02[02]: *<A.03.05.02.ODP[01]: devices or types of devices>*** are authenticated before establishing a system connection.	

03.05.03 Multi-Factor Authentication

03.05.03	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented	

03.05.03	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.05.03[01]:** multi-factor authentication for access to privileged accounts is implemented. **A.03.05.03[02]:** multi-factor authentication for access to non-privileged accounts is implemented.	

03.05.04 Replay-Resistant Authentication

03.05.04	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.05.04[01]:** replay-resistant authentication mechanisms for access to privileged accounts are implemented. **A.03.05.04[02]:** replay-resistant authentication mechanisms for access to non-privileged accounts are implemented.	

03.05.05 Identifier Management

03.05.05	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented?	

03.05.05	Control Summary Information

A.03.05.05.ODP[01]: *the time period for preventing the reuse of identifiers is defined*.

A.03.05.05.ODP[02]: *characteristics used to identify individual status are defined*.

A.03.05.05.a: authorization is received from organizational personnel or roles to assign an individual, group, role, service, or device identifier.

A.03.05.05.b[01]: an identifier that identifies an individual, group, role, service, or device is selected.

A.03.05.05.b[02]: an identifier that identifies an individual, group, role, service, or device is assigned.

A.03.05.05.c: the reuse of identifiers for ***<A.03.05.05.ODP[01]: time period>*** is prevented.

A.03.05.05.d: individual identifiers are managed by uniquely identifying each individual as ***<A.03.05.05.ODP[02]: characteristic>***.

.

03.05.07 Password Management

03.05.07	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.05.07.ODP[01]: *the frequency at which to update the list of commonly used, expected, or compromised passwords is defined*.

A.03.05.07.ODP[02]: *password composition and complexity rules are defined*.

A.03.05.07.a[01]: a list of commonly used, expected, or compromised passwords is maintained.

A.03.05.07.a[02]: a list of commonly used, expected, or compromised passwords is updated ***<A.03.05.07.ODP[01]: frequency>***.

A.03.05.07.a[03]: a list of commonly used, expected, or compromised passwords is updated when organizational passwords are suspected to have been compromised.

A.03.05.07.b: passwords are verified not to be found on the list of commonly used, expected, or compromised passwords when they are created or updated by users.

A.03.05.07.c: passwords are only transmitted over cryptographically protected channels.

A.03.05.07.d: passwords are stored in a cryptographically protected form.

A.03.05.07.e: a new password is selected upon first use after account recovery.

A.03.05.07.f: the following composition and complexity rules for passwords are enforced:

03.05.07	Control Summary Information
<A.03.05.07.ODP[02]: rules>.	

03.05.11 Authentication Feedback

03.05.11	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.05.11:** feedback of authentication information during the authentication process is obscured.	

03.05.12 Authenticator Management

03.05.12	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.05.12.ODP[01]:** *the frequency for changing or refreshing authenticators is defined*. **A.03.05.12.ODP[02]:** *events that trigger the change or refreshment of authenticators are defined*. **A.03.05.12.a:** the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution is verified. **A.03.05.12.b:** initial authenticator content for any authenticators issued by the organization is established. **A.03.05.12.c[01]:** administrative procedures for initial authenticator distribution are established. **A.03.05.12.c[02]:** administrative procedures for lost, compromised, or damaged authenticators are established.	

03.05.12	Control Summary Information

A.03.05.12.c[03]: administrative procedures for revoking authenticators are established.

A.03.05.12.c[04]: administrative procedures for initial authenticator distribution are implemented.

A.03.05.12.c[05]: administrative procedures for lost, compromised, or damaged authenticators are implemented.

A.03.05.12.c[06]: administrative procedures for revoking authenticators are implemented.

A.03.05.12.d: default authenticators are changed at first use.

A.03.05.12.e: authenticators are changed or refreshed ***<A.03.05.12.ODP[01]: frequency>*** or when the following events occur: ***<A.03.05.12.ODP[02]: events>***.

A.03.05.12.f[01]: authenticator content is protected from unauthorized disclosure.

A.03.05.12.f[02]: authenticator content is protected from unauthorized modification.

03.06 IR - Incident Response

03.06.01 Incident Handling

03.06.01	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.06.01[01]: an incident-handling capability that is consistent with the incident response plan is implemented.

A.03.06.01[02]: the incident handling capability includes preparation.

A.03.06.01[03]: the incident handling capability includes detection and analysis.

A.03.06.01[04]: the incident handling capability includes containment.

A.03.06.01[05]: the incident handling capability includes eradication.

A.03.06.01[06]: the incident handling capability includes recovery.

03.06.02 Incident Monitoring, Reporting, and Response Assistance

03.06.02	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.06.02.ODP[01]:** *the time period to report suspected incidents to the organizational incident response capability is defined*. **A.03.06.02.ODP[02]:** *authorities to whom incident information is to be reported are defined*. **A.03.06.02.a[01]:** system security incidents are tracked. **A.03.06.02.a[02]:** system security incidents are documented. **A.03.06.02.b:** suspected incidents are reported to the organizational incident response capability within ***<A.03.06.02.ODP[01]: time period>***. **A.03.06.02.c:** incident information is reported to ***<A.03.06.02.ODP[02]: authorities>***. **A.03.06.02.d:** an incident response support resource that offers advice and assistance to system users on handling and reporting incidents is provided.	

03.06.03 Incident Response Testing

03.06.03	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.06.03.ODP[01]:** *the frequency at which to test the effectiveness of the incident response capability for the system is defined.* **A.03.06.03:** the effectiveness of the incident response capability is tested ***<A.03.06.03.ODP[01]: frequency>***.	

03.06.04 Incident Response Training

03.06.04	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.06.04.ODP[01]:** *the time period within which incident response training is to be provided to system users is defined*. **A.03.06.04.ODP[02]:** *the frequency at which to provide incident response training to users after initial training is defined.* **A.03.06.04.ODP[03]:** *the frequency at which to review and update incident response training content is defined.* **A.03.06.04.ODP[04]:** *events that initiate a review of the incident response training content are defined*. **A.03.06.04.a.01:** incident response training for system users consistent with assigned roles and responsibilities is provided within ***<A.03.06.04.ODP[01]: time period>*** of assuming an incident response role or responsibility or acquiring system access. **A.03.06.04.a.02:** incident response training for system users consistent with assigned roles and responsibilities is provided when required by system changes. **A.03.06.04.a.03:** incident response training for system users consistent with assigned roles and responsibilities is provided ***<A.03.06.04.ODP[02]: frequency>*** thereafter. **A.03.06.04.b[01]:** incident response training content is reviewed ***<A.03.06.04.ODP[03]: frequency>***. **A.03.06.04.b[02]:** incident response training content is updated ***<A.03.06.04.ODP[03]: frequency>***. **A.03.06.04.b[03]:** incident response training content is reviewed following ***<A.03.06.04.ODP[04]: events>***. **A.03.06.04.b[04]:** incident response training content is updated following ***<A.03.06.04.ODP[04]: events>***.	

03.06.05 Incident Response Plan

03.06.05	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply):	

03.06.05	Control Summary Information

☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.06.05.a.01: an incident response plan is developed that provides the organization with a roadmap for implementing its incident response capability.

A.03.06.05.a.02: an incident response plan is developed that describes the structure and organization of the incident response capability.

A.03.06.05.a.03: an incident response plan is developed that provides a high-level approach for how the incident response capability fits into the overall organization.

A.03.06.05.a.04: an incident response plan is developed that defines reportable incidents.

A.03.06.05.a.05: an incident response plan is developed that addresses the sharing of incident information.

A.03.06.05.a.06: an incident response plan is developed that designates responsibilities to organizational entities, personnel, or roles.

A.03.06.05.b[01]: copies of the incident response plan are distributed to designated incident response personnel (identified by name or by role).

A.03.06.05.b[02]: copies of the incident response plan are distributed to organizational elements.

A.03.06.05.c: the incident response plan is updated to address system and organizational changes or problems encountered during plan implementation, execution, or testing.

A.03.06.05.d: the incident response plan is protected from unauthorized disclosure.

03.07 MA - Maintenance

03.07.04 Maintenance Tools

03.07.04	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

03.07.04	Control Summary Information

A.03.07.04.a[01]: the use of system maintenance tools is approved.

A.03.07.04.a[02]: the use of system maintenance tools is controlled.

A.03.07.04.a[03]: the use of system maintenance tools is monitored.

A.03.07.04.b: media with diagnostic and test programs are checked for malicious code before the media are used in the system.

A.03.07.04.c: the removal of system maintenance equipment containing CUI is prevented by verifying that there is no CUI on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility.

03.07.05 Nonlocal Maintenance

03.07.05	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.07.05.a[01]: nonlocal maintenance and diagnostic activities are approved.

A.03.07.05.a[02]: nonlocal maintenance and diagnostic activities are monitored.

A.03.07.05.b[01]: multi-factor authentication is implemented in the establishment of nonlocal maintenance and diagnostic sessions.

A.03.07.05.b[02]: replay resistance is implemented in the establishment of nonlocal maintenance and diagnostic sessions.

A.03.07.05.c[01]: session connections are terminated when nonlocal maintenance is completed.

A.03.07.05.c[02]: network connections are terminated when nonlocal maintenance is completed.

03.07.06 Maintenance Personnel

03.07.06	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented

03.07.06	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.07.06.a:** a process for maintenance personnel authorization is established. **A.03.07.06.b:** a list of authorized maintenance organizations or personnel is maintained. **A.03.07.06.c:** non-escorted personnel who perform maintenance on the system possess the required access authorizations. **A.03.07.06.d[01]:** organizational personnel with required access authorizations are designated to supervise the maintenance activities of personnel who do not possess the required access authorizations. **A.03.07.06.d[02]:** organizational personnel with required technical competence are designated to supervise the maintenance activities of personnel who do not possess the required access authorizations.	

03.08 MP - Media Protection

03.08.01 Media Storage

03.08.01	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.08.01[01]:** system media that contain CUI are physically controlled. **A.03.08.01[02]:** system media that contain CUI are securely stored.	

03.08.02 Media Access

03.08.02	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply):	

03.08.02	Control Summary Information
☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.08.02:** access to CUI on system media is restricted to authorized personnel or roles.	

03.08.03 Media Sanitization

03.08.03	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.08.03:** system media that contain CUI are sanitized prior to disposal, release out of organizational control, or release for reuse.	

03.08.04 Media Marking

03.08.04	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.08.04[01]:** system media that contain CUI are marked to indicate distribution limitations. **A.03.08.04[02]:** system media that contain CUI are marked to indicate handling caveats. **A.03.08.04[03]:** system media that contain CUI are marked to indicate applicable CUI markings.	

03.08.05 Media Transport

03.08.05	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.08.05.a[01]:** system media that contain CUI are protected during transport outside of controlled areas. **A.03.08.05.a[02]:** system media that contain CUI are controlled during transport outside of controlled areas. **A.03.08.05.b:** accountability for system media that contain CUI is maintained during transport outside of controlled areas. **A.03.08.05.c:** activities associated with the transport of system media that contain CUI are documented.	

03.08.07 Media Use

03.08.07	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.08.07.ODP[01]:** *types of system media with usage restrictions or that are prohibited from use are defined*. **A.03.08.07.a:** the use of the following types of system media is restricted or prohibited: ***<A.03.08.07.ODP[01]: types of system media>***. **A.03.08.07.b:** the use of removable system media without an identifiable owner is prohibited.	

03.08.09 System Backup - Cryptographic Protection

03.08.09	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.08.09.a:** the confidentiality of backup information is protected. **A.03.08.09.b:** cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI at backup storage locations.	

03.09 PS - Personnel Security

03.09.01 Personnel Screening

03.09.01	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.09.01.ODP[01]:** *conditions that require the rescreening of individuals are defined*. **A.03.09.01.a:** individuals are screened prior to authorizing access to the system. **A.03.09.01.b:** individuals are rescreened in accordance with the following conditions: ***<A.03.09.01.ODP[01]: conditions>***.	

03.09.02 Personnel Termination and Transfer

03.09.02	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented	

03.09.02	Control Summary Information

☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.09.02.ODP[01]: *the time period within which to disable system access is defined*.

A.03.09.02.a.01: upon termination of individual employment, system access is disabled within ***<A.03.09.02.ODP[01]: time period>***.

A.03.09.02.a.02[01]: upon termination of individual employment, authenticators associated with the individual are terminated or revoked.

A.03.09.02.a.02[02]: upon termination of individual employment, credentials associated with the individual are terminated or revoked.

A.03.09.02.a.03: upon termination of individual employment, security-related system property is retrieved.

A.03.09.02.b.01[01]: upon individual reassignment or transfer to other positions in the organization, the ongoing operational need for current logical and physical access authorizations to the system and facility is reviewed.

A.03.09.02.b.01[02]: upon individual reassignment or transfer to other positions in the organization, the ongoing operational need for current logical and physical access authorizations to the system and facility is confirmed.

A.03.09.02.b.02: upon individual reassignment or transfer to other positions in the organization, access authorization is modified to correspond with any changes in operational need.

03.10 PE - Physical Protection

03.10.01 Physical Access Authorizations

03.10.01	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.10.01.ODP[01]: *the frequency at which to review the access list detailing authorized facility*

03.10.01	Control Summary Information

access by individuals is defined.

A.03.10.01.a[01]: a list of individuals with authorized access to the facility where the system resides is developed.

A.03.10.01.a[02]: a list of individuals with authorized access to the facility where the system resides is approved.

A.03.10.01.a[03]: a list of individuals with authorized access to the facility where the system resides is maintained.

A.03.10.01.b: authorization credentials for facility access are issued.

A.03.10.01.c: the facility access list is reviewed ***<A.03.10.01.ODP[01]: frequency>***.

A.03.10.01.d: individuals from the facility access list are removed when access is no longer required.

03.10.02 Monitoring Physical Access

03.10.02	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.10.02.ODP[01]: *the frequency at which to review physical access logs is defined.*

A.03.10.02.ODP[02]: *events or potential indications of events requiring physical access logs to be reviewed are defined.*

A.03.10.02.a[01]: physical access to the facility where the system resides is monitored to detect physical security incidents.

A.03.10.02.a[02]: physical security incidents are responded to.

A.03.10.02.b[01]: physical access logs are reviewed ***<A.03.10.02.ODP[01]: frequency>***.

A.03.10.02.b[02]: physical access logs are reviewed upon occurrence of ***<A.03.10.02.ODP[02]: events or potential indications of events>***.

03.10.06 Alternate Work Site

03.10.06	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.10.06.ODP[01]:** *security requirements to be employed at alternate work sites are defined*. **A.03.10.06.a:** alternate work sites allowed for use by employees are determined. **A.03.10.06.b:** the following security requirements are employed at alternate work sites: ***<A.03.10.06.ODP[01]: security requirements>***.	

03.10.07 Physical Access Control

03.10.07	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.10.07.a.01:** physical access authorizations are enforced at entry and exit points to the facility where the system resides by verifying individual physical access authorizations before granting access. **A.03.10.07.a.02:** physical access authorizations are enforced at entry and exit points to the facility where the system resides by controlling ingress and egress with physical access control systems, devices, or guards. **A.03.10.07.b:** physical access audit logs for entry or exit points are maintained. **A.03.10.07.c[01]:** visitors are escorted. **A.03.10.07.c[02]:** visitor activity is controlled. **A.03.10.07.d:** keys, combinations, and other physical access devices are secured. **A.03.10.07.e:** physical access to output devices is controlled to prevent unauthorized individuals from obtaining access to CUI.	

03.10.08 Access Control for Transmission

03.10.08	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.10.08:** physical access to system distribution and transmission lines within organizational facilities is controlled.	

03.11 RA - Risk Assessment

03.11.01 Risk Assessment

03.11.01	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.11.01.ODP[01]:** *the frequency at which to update the risk assessment is defined.* **A.03.11.01.a:** the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed. **A.03.11.01.b:** risk assessments are updated ***<A.03.11.01.ODP[01]: frequency>***.	

03.11.02 Vulnerability Monitoring and Scanning

03.11.02	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented	

03.11.02	Control Summary Information

☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.11.02.ODP[01]: *the frequency at which the system is monitored for vulnerabilities is defined.*

A.03.11.02.ODP[02]: *the frequency at which the system is scanned for vulnerabilities is defined.*

A.03.11.02.ODP[03]: *response times to remediate system vulnerabilities are defined*.

A.03.11.02.ODP[04]: *the frequency at which to update system vulnerabilities to be scanned is defined.*

A.03.11.02.a[01]: the system is monitored for vulnerabilities ***<A.03.11.02.ODP[01]: frequency>***.

A.03.11.02.a[02]: the system is scanned for vulnerabilities ***<A.03.11.02.ODP[02]: frequency>***.

A.03.11.02.a[03]: the system is monitored for vulnerabilities when new vulnerabilities that affect the system are identified.

A.03.11.02.a[04]: the system is scanned for vulnerabilities when new vulnerabilities that affect the system are identified.

A.03.11.02.b: system vulnerabilities are remediated within ***<A.03.11.02.ODP[03]: response times>***.

A.03.11.02.c[01]: system vulnerabilities to be scanned are updated ***<A.03.11.02.ODP[04]: frequency>***.

A.03.11.02.c[02]: system vulnerabilities to be scanned are updated when new vulnerabilities are identified and reported.

03.11.04 Risk Response

03.11.04	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.11.04[01]: findings from security assessments are responded to.

A.03.11.04[02]: findings from security monitoring are responded to.

A.03.11.04[03]: findings from security audits are responded to.

03.12 CA - Security Assessment and Monitoring

03.12.01 Security Assessment

03.12.01	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.12.01.ODP[01]:** *the frequency at which to assess the security requirements for the system and its environment of operation is defined.* **A.03.12.01:** the security requirements for the system and its environment of operation are assessed ***<A.03.12.01.ODP[01]: frequency>*** to determine if the requirements have been satisfied.	

03.12.02 Plan of Action and Milestones

03.12.02	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.12.02.a.01:** a plan of action and milestones for the system is developed to document the planned remediation actions for correcting weaknesses or deficiencies noted during security assessments. **A.03.12.02.a.02:** a plan of action and milestones for the system is developed to reduce or eliminate known system vulnerabilities. **A.03.12.02.b.01:** the existing plan of action and milestones is updated based on the findings from security assessments. **A.03.12.02.b.02:** the existing plan of action and milestones is updated based on the findings from audits or reviews.	

03.12.02	Control Summary Information
A.03.12.02.b.03: the existing plan of action and milestones is updated based on the findings from continuous monitoring activities.	

03.12.03 Continuous Monitoring

03.12.03	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.12.03[01]:** a system-level continuous monitoring strategy is developed. **A.03.12.03[02]:** a system-level continuous monitoring strategy is implemented. **A.03.12.03[03]:** ongoing monitoring is included in the continuous monitoring strategy. **A.03.12.03[04]:** security assessments are included in the continuous monitoring strategy.	

03.12.05 Information Exchange

03.12.05	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.12.05.ODP[01]:** *one or more of the following PARAMETER VALUES are selected: {interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements*; *other types of agreements}.* **A.03.12.05.ODP[02]:** *the frequency at which to review and update agreements is defined.*	

03.12.05	Control Summary Information

A.03.12.05.a[01]: the exchange of CUI between the system and other systems is approved using ***<A.03.12.05.ODP[01]: SELECTED PARAMETER VALUES>***.

A.03.12.05.a[02]: the exchange of CUI between the system and other systems is managed using ***<A.03.12.05.ODP[01]: SELECTED PARAMETER VALUES>***.

A.03.12.05.b[01]: interface characteristics for each system are documented as part of the exchange agreements.

A.03.12.05.b[02]: security requirements for each system are documented as part of the exchange agreements.

A.03.12.05.b[03]: responsibilities for each system are documented as part of the exchange agreements.

A.03.12.05.c[01]: exchange agreements are reviewed ***<A.03.12.05.ODP[02]: frequency>***.

A.03.12.05.c[02]: exchange agreements are updated ***<A.03.12.05.ODP[02]: frequency>***.

03.13 SC - System and Communications Protection

03.13.01 Boundary Protection

03.13.01	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.13.01.a[01]: communications at external managed interfaces to the system are monitored.

A.03.13.01.a[02]: communications at external managed interfaces to the system are controlled.

A.03.13.01.a[03]: communications at key internal managed interfaces within the system are monitored.

A.03.13.01.a[04]: communications at key internal managed interfaces within the system are controlled.

A.03.13.01.b: subnetworks are implemented for publicly accessible system components that are physically or logically separated from internal networks.

A.03.13.01.c: external system connections are only made through managed interfaces that consist of

03.13.01	Control Summary Information
boundary protection devices arranged in accordance with an organizational security architecture.	

03.13.04 Information in Shared System Resources

03.13.04	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.13.04[01]:** unauthorized information transfer via shared system resources is prevented. **A.03.13.04[02]:** unintended information transfer via shared system resources is prevented.	

03.13.06 Network Communications - Deny by Default - Allow by Exception

03.13.06	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.13.06[01]:** network communications traffic is denied by default. **A.03.13.06[02]:** network communications traffic is allowed by exception.	

03.13.08 Transmission and Storage Confidentiality

03.13.08	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.13.08[01]:** cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI during transmission. **A.03.13.08[02]:** cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI while in storage.	

03.13.09 Network Disconnect

03.13.09	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? ***A.03.13.09.ODP[01]:*** *the time period of inactivity after which the system terminates a network connection associated with a communications session is defined.* ***A.03.13.09:*** *the network connection associated with a communications session is terminated at the end of the session or after* ***<A.03.13.09.ODP[01]: time period>*** *of inactivity.*	

03.13.10 Cryptographic Key Establishment and Management

03.13.10	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned	

03.13.10	Control Summary Information
☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.13.10.ODP[01]:** *requirements for key generation, distribution, storage, access, and destruction are defined.* **A.03.13.10[01]:** cryptographic keys are established in the system in accordance with the following key management requirements: ***<A.03.13.10.ODP[01]: requirements>***. **A.03.13.10[02]:** cryptographic keys are managed in the system in accordance with the following key management requirements: ***<A.03.13.10.ODP[01]: requirements>***.	

03.13.11 Cryptographic Protection

03.13.11	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.13.11.ODP[01]:** *the types of cryptography for protecting the confidentiality of CUI are defined*. **A.03.13.11:** the following types of cryptography are implemented to protect the confidentiality of CUI: ***<A.03.13.11.ODP[01]: types of cryptography>***.	

03.13.12 Collaborative Computing Devices and Applications

03.13.12	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented?	

03.13.12	Control Summary Information

A.03.13.12.ODP[01]: *exceptions where remote activation is to be allowed are defined.*

A.03.13.12.a: the remote activation of collaborative computing devices and applications is prohibited with the following exceptions: ***<A.03.13.12.ODP[01]: exceptions>***.

A.03.13.12.b: an explicit indication of use is provided to users who are physically present at the devices.

03.13.13 Mobile Code

03.13.13	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.13.13.a[01]: acceptable mobile code is defined.

A.03.13.13.a[02]: acceptable mobile code technologies are defined.

A.03.13.13.b[01]: the use of mobile code is authorized.

A.03.13.13.b[02]: the use of mobile code is monitored.

A.03.13.13.b[03]: the use of mobile code is controlled.

03.13.15 Session Authenticity

03.13.15	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

03.13.15	Control Summary Information
A.03.13.15: the authenticity of communications sessions is protected.	

03.14 SI - System and Information Integrity

03.14.01 Flaw Remediation

03.14.01	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.14.01.ODP[01]:** *the time period within which to install security-relevant software updates after the release of the updates is defined*. **A.03.14.01.ODP[02]:** *the time period within which to install security-relevant firmware updates after the release of the updates is defined.* **A.03.14.01.a[01]:** system flaws are identified. **A.03.14.01.a[02]:** system flaws are reported. **A.03.14.01.a[03]:** system flaws are corrected. **A.03.14.01.b[01]:** security-relevant software updates are installed within ***<A.03.14.01.ODP[01]: time period>*** of the release of the updates. **A.03.14.01.b[02]:** security-relevant firmware updates are installed within ***<A.03.14.01.ODP[02]: time period>*** of the release of the updates.	

03.14.02 Malicious Code Protection

03.14.02	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned	

03.14.02	Control Summary Information

☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.14.02.ODP[01]: *the frequency at which malicious code protection mechanisms perform scans is defined*.

A.03.14.02.a[01]: malicious code protection mechanisms are implemented at system entry and exit points to detect malicious code.

A.03.14.02.a[02]: malicious code protection mechanisms are implemented at system entry and exit points to eradicate malicious code.

A.03.14.02.b: malicious code protection mechanisms are updated as new releases are available in accordance with configuration management policy and procedures.

A.03.14.02.c.01[01]: malicious code protection mechanisms are configured to perform scans of the system ***<A.03.14.02.ODP[01]: frequency>***.

A.03.14.02.c.01[02]: malicious code protection mechanisms are configured to perform real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed.

A.03.14.02.c.02: malicious code protection mechanisms are configured to block malicious code, quarantine malicious code, or take other actions in response to malicious code detection.

03.14.03 Security Alerts, Advisories, and Directives

03.14.03	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.14.03.a: system security alerts, advisories, and directives from external organizations are received on an ongoing basis.

A.03.14.03.b[01]: internal security alerts, advisories, and directives are generated, as necessary.

A.03.14.03.b[02]: internal security alerts, advisories, and directives are disseminated, as necessary.

03.14.06 System Monitoring

03.14.06	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.14.06.a.01[01]:** the system is monitored to detect attacks. **A.03.14.06.a.01[02]:** the system is monitored to detect indicators of potential attacks. **A.03.14.06.a.02:** the system is monitored to detect unauthorized connections. **A.03.14.06.b:** unauthorized use of the system is identified. **A.03.14.06.c[01]:** inbound communications traffic is monitored to detect unusual or unauthorized activities or conditions. **A.03.14.06.c[02]:** outbound communications traffic is monitored to detect unusual or unauthorized activities or conditions.	

03.14.08 Information Management and Retention

03.14.08	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.14.08[01]:** CUI within the system is managed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements. **A.03.14.08[02]:** CUI within the system is retained in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements. **A.03.14.08[03]:** CUI output from the system is managed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements. **A.03.14.08[04]:** CUI output from the system is retained in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	

03.14.08	Control Summary Information

03.15 Planning

03.15.01 Policy and Procedures

03.15.01	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.15.01.ODP[01]: *the frequency at which the policies and procedures for satisfying security requirements are reviewed and updated is defined.*

A.03.15.01.a[01]: policies needed to satisfy the security requirements for the protection of CUI are developed and documented.

A.03.15.01.a[02]: policies needed to satisfy the security requirements for the protection of CUI are disseminated to organizational personnel or roles.

A.03.15.01.a[03]: procedures needed to satisfy the security requirements for the protection of CUI are developed and documented.

A.03.15.01.a[04]: procedures needed to satisfy the security requirements for the protection of CUI are disseminated to organizational personnel or roles.

A.03.15.01.b[01]: policies and procedures are reviewed ***<A.03.15.01.ODP[01]: frequency>***.

A.03.15.01.b[02]: policies and procedures are updated ***<A.03.15.01.ODP[01]: frequency>***.

03.15.02 System Security Plan

03.15.02	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation

03.15.02	Control Summary Information

☐ Not applicable

What is the solution and how is it implemented?

A.03.15.02.ODP[01]: *the frequency at which the system security plan is reviewed and updated is defined.*

A.03.15.02.a.01: a system security plan that defines the constituent system components is developed.

A.03.15.02.a.02: a system security plan that identifies the information types processed, stored, and transmitted by the system is developed.

A.03.15.02.a.03: a system security plan that describes specific threats to the system that are of concern to the organization is developed.

A.03.15.02.a.04: a system security plan that describes the operational environment for the system and any dependencies on or connections to other systems or system components is developed.

A.03.15.02.a.05: a system security plan that provides an overview of the security requirements for the system is developed.

A.03.15.02.a.06: a system security plan that describes the safeguards in place or planned for meeting the security requirements is developed.

A.03.15.02.a.07: a system security plan that identifies individuals that fulfill system roles and responsibilities is developed.

A.03.15.02.a.08: a system security plan that includes other relevant information necessary for the protection of CUI is developed.

A.03.15.02.b[01]: the system security plan is reviewed ***<A.03.15.02.ODP[01]: frequency>***.

A.03.15.02.b[02]: the system security plan is updated ***<A.03.15.02.ODP[01]: frequency>***.

A.03.15.02.c: the system security plan is protected from unauthorized disclosure.

03.15.03 Rules of Behavior

03.15.03	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.15.03.ODP[01]: *the frequency at which the rules of behavior are reviewed and updated is defined.*

A.03.15.03.a: rules that describe responsibilities and expected behavior for system usage and

03.15.03	Control Summary Information
protecting CUI are established. **A.03.15.03.b:** rules are provided to individuals who require access to the system. **A.03.15.03.c:** a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior is received before authorizing access to CUI and the system. **A.03.15.03.d[01]:** the rules of behavior are reviewed ***<A.03.15.03.ODP[01]: frequency>***. **A.03.15.03.d[02]:** the rules of behavior are updated ***<A.03.15.03.ODP[01]: frequency>***.	

03.16 System and Services Acquisition

03.16.01 Policy and Procedures

03.16.01	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.16.01.ODP[01]:** *systems security engineering principles to be applied to the development or modification of the system and system components are defined.* **A.03.16.01:** ***<A.03.16.01.ODP[01]: systems security engineering principles>*** are applied to the development or modification of the system and system components.	

03.16.02 Unsupported System Components

03.16.02	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented	

03.16.02	Control Summary Information

☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.16.02.a: system components are replaced when support for the components is no longer available from the developer, vendor, or manufacturer.

A.03.16.02.b: options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced are provided.

03.16.03 External System Services

03.16.03	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A.03.16.03.ODP[01]: ***security requirements to be satisfied by external system service providers are defined*****.**

A.03.16.03.a: the providers of external system services used for the processing, storage, or transmission of CUI comply with the following security requirements: ***<A.03.16.03.ODP[01]: security requirements>***.

A.03.16.03.b: user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers, are defined and documented.

A.03.16.03.c: processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis are implemented.

03.17 Supply Chain Risk Management

03.17.01 Supply Chain Risk Management Plan

03.17.01	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.17.01.ODP[01]:** *the frequency at which to review and update the supply chain risk management plan is defined.* **A.03.17.01.a[01]:** a plan for managing supply chain risks is developed. **A.03.17.01.a[02]:** the SCRM plan addresses risks associated with the research and development of the system, system components, or system services. **A.03.17.01.a[03]:** the SCRM plan addresses risks associated with the design of the system, system components, or system services. **A.03.17.01.a[04]:** the SCRM plan addresses risks associated with the manufacturing of the system, system components, or system services. **A.03.17.01.a[05]:** the SCRM plan addresses risks associated with the acquisition of the system, system components, or system services. **A.03.17.01.a[06]:** the SCRM plan addresses risks associated with the delivery of the system, system components, or system services. **A.03.17.01.a[07]:** the SCRM plan addresses risks associated with the integration of the system, system components, or system services. **A.03.17.01.a[08]:** the SCRM plan addresses risks associated with the operation of the system, system components, or system services. **A.03.17.01.a[09]:** the SCRM plan addresses risks associated with the maintenance of the system, system components, or system services. **A.03.17.01.a[10]:** the SCRM plan addresses risks associated with the disposal of the system, system components, or system services. **A.03.17.01.b[01]:** the SCRM plan is reviewed ***<A.03.17.01.ODP[01]: frequency>*.** **A.03.17.01.b[02]:** the SCRM plan is updated ***<A.03.17.01.ODP[01]: frequency>*.** **A.03.17.01.c:** the SCRM plan is protected from unauthorized disclosure.	

03.17.02 Acquisition Strategies, Tools, and Methods

03.17.02	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.17.02[01]:** acquisition strategies, contract tools, and procurement methods are developed to identify supply chain risks. **A.03.17.02[02]:** acquisition strategies, contract tools, and procurement methods are developed to protect against supply chain risks. **A.03.17.02[03]:** acquisition strategies, contract tools, and procurement methods are developed to mitigate supply chain risks. **A.03.17.02[04]:** acquisition strategies, contract tools, and procurement methods are implemented to identify supply chain risks. **A.03.17.02[05]:** acquisition strategies, contract tools, and procurement methods are implemented to protect against supply chain risks. **A.03.17.02[06]:** acquisition strategies, contract tools, and procurement methods are implemented to mitigate supply chain risks.	

03.17.03 Supply Chain Requirements and Processes

03.17.03	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? **A.03.17.03.ODP[01]:** *security requirements to protect against supply chain risks to the system, system*	

03.17.03	Control Summary Information

components, or system services and to limit the harm or consequences from supply chain-related events are defined.

A.03.17.03.a[01]: a process for identifying weaknesses or deficiencies in the supply chain elements and processes is established.

A.03.17.03.a[02]: a process for addressing weaknesses or deficiencies in the supply chain elements and processes is established.

A.03.17.03.b: the following security requirements are enforced to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences of supply chain-related events: ***<A.03.17.03.ODP[01]: security requirements>***.

10 Template Revision History

This is the revision history of this template. This section can be removed once you've completed your document.

Version	Date	Author	Description
1.0	19-NOV-2024	Lbowser <Laura Raderman>	Initial Document for 800-171r3