1. SYSTEM IDENTIFICATION

1.1. System Name/Title: [State the name of the system. Spell out acronyms.]

1.1.1.   System Categorization: Moderate Impact for Confidentiality

1.1.2.   System Unique Identifier: [Insert the System Unique Identifier]

1.2. Responsible Organization:

Name:	
Address:	
Phone:	

1.2.1.   Information Owner (Government point of contact responsible for providing and/or receiving CUI)**:**

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.2.1.1. System Owner (assignment of security responsibility)**:**

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.2.1.2. System Security Officer:

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.3. General Description/Purpose of System: What is the function/purpose of the system? **[Provide a short, high-level description of the function/purpose of the system.**]

1.3.1.   Number of end users and privileged users: **[In the table below, provide the *approximate* number of users and administrators of the system. Include all those with privileged access such as system administrators, database administrators, application administrators, etc. Add rows to define different roles as needed.**]

Roles of Users and Number of Each Type:

Number of Users	Number of Administrators/ Privileged Users

1.4. General Description of Information: CUI information types processed, stored, or transmitted by the system are determined and documented. For more information, see the CUI Registry at https://www.archives.gov/cui/registry/category-list. [**Document the CUI information types processed, stored, or transmitted by the system below**].

2. SYSTEM ENVIRONMENT

Include a <u>detailed</u> topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note**:** *this does not require depicting every workstation or desktop*, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram.
[**Insert a system topology graphic. Provide a narrative consistent with the graphic that clearly lists and describes each system component.**]

2.1. Include or reference a **complete and accurate** listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component. [**Insert the reference/URL or note that the hardware component inventory is attached.**]

2.2. List all software components installed on the system. [**Insert the reference/URL or note that the software component inventory is attached.**]

2.3. Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization? [**Yes/No - If no, explain:**]

3. REQUIREMENTS

(Note: The source of the requirements is NIST Special Publication 800-171, dated December 2016)

Provide a thorough description of how all of the security requirements are being implemented or planned to be implemented. The description for each security requirement contains: 1) the security requirement number and description; 2) how the security requirement is being implemented or planned to be implemented; and 3) any scoping guidance that has been applied (e.g., compensating mitigations(s) in place due to implementation constraints in lieu of the stated requirement). If the requirement is not applicable to the system, provide rationale.

3.1. Access Control

3.1.1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.2. Limit system access to the types of transactions and functions that authorized users are permitted to execute.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.3. Control the flow of CUI in accordance with approved authorizations.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.4. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.5. Employ the principle of least privilege, including for specific security functions and privileged accounts.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.6. Use non-privileged accounts or roles when accessing nonsecurity functions.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.7. Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.8. Limit unsuccessful logon attempts.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.9. Provide privacy and security notices consistent with applicable CUI rules.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.10. Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.11. Terminate (automatically) a user session after a defined condition.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.12. Monitor and control remote access sessions.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.13. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.14. Route remote access via managed access control points.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.15. Authorize remote execution of privileged commands and remote access to security-relevant information.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.16. Authorize wireless access prior to allowing such connections.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.17. Protect wireless access using authentication and encryption.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.18. Control connection of mobile devices.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.19. Encrypt CUI on mobile devices and mobile computing platforms.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.20. Verify and control/limit connections to and use of external systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.21. Limit use of organizational portable storage devices on external systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.22. Control CUI posted or processed on publicly accessible systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.2. Awareness and Training

3.2.1. Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.2.2. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.2.3. Provide security awareness training on recognizing and reporting potential indicators of insider threat.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3. Audit and Accountability

3.3.1. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.2. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.3. Review and update logged events.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.4. Alert in the event of an audit logging process failure.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.5. Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.6. Provide audit record reduction and report generation to support on-demand analysis and reporting.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.7. Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.8. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.9. Limit management of audit logging functionality to a subset of privileged users.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4. Audit and Accountability

3.4.1. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.2. Establish and enforce security configuration settings for information technology products employed in organizational systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.3. Track, review, approve or disapprove, and log changes to organizational systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.4. Analyze the security impact of changes prior to implementation.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.5. Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.6. Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.7. Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.8. Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.9. Control and monitor user-installed software.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5. Identification and Authentication

3.5.1. Identify system users, processes acting on behalf of users, and devices.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.2. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.3. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.4. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.5.   Prevent reuse of identifiers for a defined period.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.6.   Disable identifiers after a defined period of inactivity.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.7.   Enforce a minimum password complexity and change of characters when new passwords are created.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.8.   Prohibit password reuse for a specified number of generations.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.9.   Allow temporary password use for system logons with an immediate change to a permanent password.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.10. Store and transmit only cryptographically-protected passwords.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.11. Obscure feedback of authentication information.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6. Incident Response

3.6.1. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6.2. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6.3. Test the organizational incident response capability

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7. Maintenance

3.7.1. Perform maintenance on organizational systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7.2. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7.3. Ensure equipment removed for off-site maintenance is sanitized of any CUI.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7.4. Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7.5. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7.6. Supervise the maintenance activities of maintenance personnel without required access authorization.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8. Media Protection

3.8.1. Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.2. Limit access to CUI on system media to authorized users.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.3. Sanitize or destroy system media containing CUI before disposal or release for reuse.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.4. Mark media with necessary CUI markings and distribution limitations.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.5. Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.6. Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.7. Control the use of removable media on system components.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.8. Prohibit the use of portable storage devices when such devices have no identifiable owner.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.9. Protect the confidentiality of backup CUI at storage locations.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.9. Personnel Security

3.9.1. Screen individuals prior to authorizing access to organizational systems containing CUI.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.9.2. Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.   Physical Protection

3.10.1. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.2. Protect and monitor the physical facility and support infrastructure for organizational systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.3. Escort visitors and monitor visitor activity.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.4. Maintain audit logs of physical access.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.5. Control and manage physical access devices.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.6. Enforce safeguarding measures for CUI at alternate work sites.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.11.   Risk Assessment

3.11.1. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.11.2. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.11.3. Remediate vulnerabilities in accordance with risk assessments.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.   Security Assessment

3.12.1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.4. Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.   System and Communications Protection

3.13.1. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.2. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.3. Separate user functionality from system management functionality.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.4. Prevent unauthorized and unintended information transfer via shared system resources.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.5. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.6. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.7. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.8. Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.9. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.10. Establish and manage cryptographic keys for cryptography employed in organizational systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.11. Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.12. Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.13. Control and monitor the use of mobile code.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.14. Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.15. Protect the authenticity of communications sessions.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.16. Protect the confidentiality of CUI at rest.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.   System and Information Integrity

3.14.1. Identify, report, and correct system flaws in a timely manner.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.2. Provide protection from malicious code at designated locations within organizational systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.3. Monitor system security alerts and advisories and take action in response.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.4. Update malicious code protection mechanisms when new releases are available.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.5. Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.6. Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.7. Identify unauthorized use of organizational systems.

☐ Implemented   ☐ Planned to be Implemented   ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

4. RECORD OF CHANGES

Date	Description	Made By:

Controlled Unclassified Information Plan of Action for [SYSTEM NAME]

Weaknesses	Responsible Office/ Organization	Resource Estimate (funded/ unfunded/ reallocation)	Scheduled Completion Date	Milestones with Interim Completion Dates	Changes to Milestones	How was the weakness identified?	Status (Ongoing or Complete)