|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version: {VERSION}****eMASS# {EMASS#}****Confidentiality: {CONFIDENTIALITY}****Integrity: {INTEGRITY}****Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **Information System Maintenance Plan****Document Version: 1.0.0****{DATE}** |
| Prepared by: {ORGANIZATION}**DISTRIBUTION IS LIMITED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS.****OTHER REQUESTS FOR THIS DOCUMENT MUST BE REFERRED TO:** {ORGANIZATION} |

**Change Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Changes Made / Section(s) |
| {DATE} | 1.0.0 | {ORGANIZATION} | Initial Document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

[1.0 OVERVIEW 1](#_Toc433348997)

[2.0 MAINTENANCE POLICY 1](#_Toc433348998)

[2.1 Purpose 1](#_Toc433348999)

[2.2 Scope 1](#_Toc433349000)

[2.3 Roles and Responsibilities 1](#_Toc433349001)

[2.4 Coordination 2](#_Toc433349002)

[3.0 MAINTENANCE PROCEDURES 2](#_Toc433349003)

[3.1 Types of Maintenance 2](#_Toc433349004)

[3.1.1 Preventive Maintenance 2](#_Toc433349005)

[3.1.2 Controlled Maintenance 2](#_Toc433349006)

[3.1.3 Corrective Maintenance 2](#_Toc433349007)

[3.2 Maintenance Tools 3](#_Toc433349008)

[3.3 Verification of Security Features 3](#_Toc433349009)

[3.4 Sanitization 3](#_Toc433349010)

[4.0 NONLOCAL MAINTENANCE 3](#_Toc433349011)

[4.1 Audit 3](#_Toc433349012)

[4.2 Authentication 3](#_Toc433349013)

[4.3 Authorization 3](#_Toc433349014)

[4.4 Records 3](#_Toc433349015)

[4.5 Connectivity 3](#_Toc433349016)

[4.6 Sanitization 4](#_Toc433349017)

[5.0 MAINTENANCE SUPPORT 4](#_Toc433349018)

[APPENDIX A – DETAILED COMPLIANCE MATRIX 5](#_Toc433349019)

[ENCLOSURE 1 – AUTHORIZED MAINTENANCE PERSONNEL 32](#_Toc433349020)

[ENCLOSURE 2 – AUTHORIZED THIRD PARTY MAINTENANCE PERSONNEL 34](#_Toc433349021)

[ENCLOSURE 3 – MAINTENANCE SUPPORT FOR SYSTEM COMPONENTS 36](#_Toc433349022)

[ENCLOSURE 4 – MAINTENANCE LOG 38](#_Toc433349023)

[Table 1 - SP-800-53v4 Compliance Matrix 1](#_Toc433274403)

[Table 2 - Roles and Responsibilities 2](#_Toc433274404)

# **OVERVIEW**

Information systems must have security controls in place to protect the maintenance activities that enable the system to function correctly. Maintenance activities include diagnosing and correcting hardware, firmware, and software problems; loading, maintaining, and updating software, device drivers, configuration settings, etc., and maintaining a historical record of system changes. Such activities may be conducted in-house or by individuals communicating through an external, non-organization controlled network (e.g., the Internet) further exposing systems to attack.

This plan ensures that {ACRONYM} maintenance, diagnostic, and repair activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location, are managed and monitored to preserve the confidentiality, integrity, and availability of {ACRONYM} information system resources.

This document complies with the following requirements from NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations". A detailed compliance matrix can be found in [Appendix A, “Detailed Compliance Matrix”](#_APPENDIX_I_–).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CNTL NO. | CONTROL NAME | PRIORITY | LOW | MOD | HIGH |
| [MA-1](#MA1) | System Maintenance Policy and Procedures | P1 | MA-1 | MA-1 | MA-1 |
| [MA-2](#MA2) | Controlled Maintenance | P2 | MA-2 | MA-2 | MA-2 (2) |
| [MA-3](#MA3) | Maintenance Tools | P3 | Not Selected | MA-3 (1) (2) | MA-3 (1) (2) (3) |
| [MA-4](#MA4) | Nonlocal Maintenance | P2 | MA-4 | MA-4 (2) | MA-4 (2) (3) |
| [MA-5](#MA5) | Maintenance Personnel | P2 | MA-5 | MA-5 | MA-5 (1) |
| [MA-6](#MA6) | Timely Maintenance | P2 | Not Selected | MA-6 | MA-6 |

Table - SP-800-53v4 Compliance Matrix

# **2.0 MAINTENANCE POLICY**

## **2.1 Purpose**

{ACRONYM} shall ensure all maintenance, diagnostic, and repair activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location, are managed and monitored to preserve the confidentiality, integrity, and availability of {ACRONYM}’s information systems.

## **2.2 Scope**

This Information System Maintenance Plan applies to {ACRONYM} and its components.

## **2.3 Roles and Responsibilities**

| Role | Responsibility |
| --- | --- |
| System Owner | 1. Control all maintenance activities
2. Ensure that personnel performing maintenance on the information system have required access authorizations
3. Explicitly approve the removal of information system or system components from organizational facilities for off-site maintenance or repairs
 |
| System Administrator | 1. Schedule, perform, document, and review records on maintenance
2. Sanitize equipment prior to offsite maintenance
3. Checks security controls following maintenance
4. Maintain system maintenance records
5. Maintain a list of authorized maintenance personnel including third-party maintenance providers.
6. Inspect all maintenance tools brought into a facility by maintenance personnel for obvious improper modifications
7. Check all diagnostic and test program media for malicious code before use
 |
| Information System Security Officer | 1. Sanitize equipment prior to offsite maintenance
2. Checks security controls following maintenance
3. Ensure that personnel performing maintenance on the information system have required access authorizations
4. Maintain a list of authorized maintenance personnel including third-party maintenance providers.
5. Inspect all maintenance tools brought into a facility by maintenance personnel for obvious improper modifications
6. Check all diagnostic and test program media for malicious code before use
 |

Table - Roles and Responsibilities

## **2.4 Coordination**

The System Owner is responsible for coordinating all maintenance activities within the {ACRONYM} and with any external, third-party vendors. In addition, the System Owner will ensure coordination with other internal entities such as the Configuration Control Board.

# **3.0 MAINTENANCE PROCEDURES**

## **3.1 Types of Maintenance**

### **3.1.1 Preventive Maintenance**

Preventive maintenance is used to ensure maximum reliability of data center equipment by providing systematic inspections, detection and correction of incipient failures, either before they occur or before they develop into major defects that result in costly downtime. Preventive maintenance can include activities such as inspections, tests, measurements, adjustments, parts replacement, and general housekeeping practices.

### **3.1.2 Controlled Maintenance**

Controlled maintenance is performed on an information system or components (software or hardware) which are scheduled and performed in accordance with manufacturer, vendor or agency specifications.

### **3.1.3 Corrective Maintenance**

Corrective maintenance occurs when a system abruptly fails or generates an error condition a corrective maintenance task is performed to repair or replace failed components (software or hardware) so the system can be restored to an operational condition as soon as possible. Corrective maintenance may be performed by in-house personnel or outside vendors under a service agreement.

## **3.2 Maintenance Tools**

Information system maintenance tools carried into a facility by personnel for usage on {ACRONYM} systems must be checked for obvious improper modifications. Media containing diagnostics software must be scanned for malicious code (e.g. virus, malware, Trojan) before the media is utilized as part of maintenance and repair activities.

## **3.3 Verification of Security Features**

After maintenance is performed, the system will be assessed utilizing the Assured Compliance Assessment Solution (ACAS), DISA Security Technical Implementation Guide (STIG) and Security Content Automation Protocol (SCAP) tools to determine if maintenance activities introduced any vulnerabilities. Specific attention will be given to new account creation, modified groups and introduction of new remote access capabilities. The maintenance activity is not considered complete until this action is performed.

## **3.4 Sanitization**

The Media Protection Plan will be followed to ensure a process that renders access to target data on the media infeasible for a given level of effort.

# **4.0 NONLOCAL MAINTENANCE**

Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network.

Does {ACRONYM} perform nonlocal maintenance?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

 If yes, complete Sections 4.1 – 4.6

If no, replace the test in Sections 4.1 – 4.6 with, “N/A – nonlocal maintenance is not performed.”

## **4.1 Audit**

The ISSO will ensure that auditing is set per STIG requirements and the security event log is reviewed immediately after maintenance is performed.

Does {ACRONYM} implement auditing per the STIG and is it reviewed after maintenance is performed?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

## **4.2 Authentication**

Any non-local system maintenance must be approved by the system owner and employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions. If password-based authentication is used during remote maintenance of {ACRONYM} systems, passwords must be changed following each remote maintenance service.

Does {ACRONYM} approve nonlocal maintenance?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

If yes, are strong passwords utilized?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

If yes, are passwords changed after maintenance is performed?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

## **4.3 Authorization**

Maintenance personnel must either have the required access authorizations or be supervised by designated {ACRONYM} personnel with the required access authorizations. Individuals supervising maintenance personnel must be technically competent in order to supervise information system maintenance.

Do maintenance have required access, or supervised?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

If yes, are supervisors technically competent?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

## **4.4 Records**

All nonlocal maintenance will be documented utilizing the form provided in [Enclosure 2, “Authorized Third Party Maintenance Personnel”](#_ENCLOSURE_2_–_1) and [Enclosure 4, “Maintenance Log”](#_ENCLOSURE_4_–).

Do maintenance records exist?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

## **4.5 Connectivity**

In the event remote connectivity is used to perform maintenance, the enclave boundary defense will be specifically configured to allow only the authorized external IP Address inbound connectivity. Credentials will only be given for the asset on which maintenance is performed. Immediately after maintenance is performed, all remote access will be terminated. All access will be implemented utilizing technologies that meet FIP 140-2 encryption requirements.

Is remote connectivity used to establish nonlocal maintenance sessions?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

If yes, are only authorized IP Addresses permitted?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

If yes, is FIPS 140-2 encryption used to establish remote sessions?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

If yes, are sessions terminated after maintenance is completed?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

## **4.6 Sanitization**

{ACRONYM} information assets or system components must not be moved off-site from facilities for maintenance or repairs without approval from the system owner. Prior to removal from facilities for off-site maintenance or repairs equipment must be sanitized to remove all information from associated media. Following any maintenance activity security controls must be checked to verify functionality.

Are {ACRONYM} assets or components moved offsite for maintenance or repairs?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

If yes, did the {ACRONYM} authorize the repairs?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

If yes, was all information sanitized prior to shipping?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

# **5.0 MAINTENANCE SUPPORT**

Maintenance Support, including parts and spares is important to ensure the availability of the {ACRONYM} systems.

Are personnel available to support the information system within 24 hours of failure?

|  |
| --- |
|[ ]  No |
|[ ]  Yes |

Are spares/parts available to support the information system within 24 hours of failure?

|  |
| --- |
|[ ]  No |
|[ ]  Yes*System Components are listed in Enclosure 3, “Maintenance Support for System Components”* |

# **APPENDIX A – DETAILED COMPLIANCE MATRIX**

The following table provides traceability between this document and the Assessment Procedures contained within NIST Special Publication 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations".

| Control Number | Assessment Number | CCI | Confidentiality | Integrity | Availability | Assessment Procedures | Reference |
| --- | --- | --- | --- | --- | --- | --- | --- |
| MA-1 | MA-1 (a) | CCI-002861 | HighModerateLow | HighModerateLow | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system. | Automatically compliant with this CCI because they are covered at the DoD level |
| MA-1 | MA-1 (a) | CCI-002862 | HighModerateLow | HighModerateLow | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system. | Automatically compliant with this CCI because they are covered at the DoD level |
| MA-1 | MA-1 (a) (1) | CCI-000852 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented maintenance policy to ensure the organization being inspected/assessed develops and documents a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. | [Section 2](#_2.0_MAINTENANCE_POLICY) |
| MA-1 | MA-1 (a) (1) | CCI-000853 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the maintenance policy via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated to the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system. | External Link |
| MA-1 | MA-1 (a) (2) | CCI-000856 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment examines the maintenance procedures via the inspected organization's information sharing capability (e.g. portal, intranet, email, etc.) to ensure it has been disseminated to the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system.  DoD has defined the personnel or roles as the SCA, ISSO, and maintenance personnel as needed by role in maintaining the system. | External Link |
| MA-1 | MA-1 (a) (2) | CCI-000855 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the Security Plan to ensure maintenance procedures are documented and are developed IAW maintenance policy provided in DoDI 8500.01..  | [Section 3](#_3.0_MAINTENANCE_PROCEDURES) |
| MA-1 | MA-1 (b) (1) | CCI-000854 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the maintenance policy to ensure review is occurring every 5 years and updates are made as necessary.DoD has defined the frequency as every 5 years. | [Change Record](#ChangeRecord) |
| MA-1 | MA-1 (b) (1) | CCI-000851 | HighModerateLow | HighModerateLow | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years. | Automatically compliant with this CCI because they are covered at the DoD level |
| MA-1 | MA-1 (b) (2) | CCI-000857 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the maintenance procedures to ensure annual review and necessary updates are occurring.  DoD has defined the frequency as annually. | [Change Record](#ChangeRecord) |
| MA-1 | MA-1 (b) (2) | CCI-001628 | HighModerateLow | HighModerateLow | HighModerateLow | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| MA-2 (2) | MA-2 (2) (a) | CCI-002863 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documentation of automated mechanisms to ensure the organization being inspected/assessed employs automated mechanisms to schedule, conduct, and document repairs. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MA-2 (2) | MA-2 (2) (a) | CCI-002905 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documentation of automated mechanisms to ensure the organization being inspected/assessed employs automated mechanisms to schedule, conduct, and document maintenance. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MA-2 (2) | MA-2 (2) (b) | CCI-002864 | High | High | High | The organization conducting the inspection/assessment obtains and examines the records of maintenance to ensure the organization being inspected/assessed produces up-to date, accurate, and complete records of all maintenance requested, scheduled, in process, and completed. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MA-2 (2) | MA-2 (2) (b) | CCI-002865 | High | High | High | The organization conducting the inspection/assessment obtains and examines the records of repair actions to ensure the organization being inspected/assessed produces up-to date, accurate, and complete records of all repair actions requested, scheduled, in process, and completed. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MA-2 | MA-2 (a) | CCI-002870 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the record of repairs to ensure the organization being inspected/assessed schedules repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. | [Section 3.1.2](#_3.1.2_Controlled_Maintenance)[Enclosure 4](#_ENCLOSURE_4_–) |
| MA-2 | MA-2 (a) | CCI-002866 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the record of maintenance to ensure the organization being inspected/assessed schedules maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. | [Enclosure 4](#_ENCLOSURE_4_–) |
| MA-2 | MA-2 (a) | CCI-002872 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines documentation of repairs to ensure the organization being inspected/assessed documents repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. | [Enclosure 4](#_ENCLOSURE_4_–) |
| MA-2 | MA-2 (a) | CCI-002868 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines documentation of maintenance to ensure the organization being inspected/assessed documents maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. | [Enclosure 4](#_ENCLOSURE_4_–) |
| MA-2 | MA-2 (a) | CCI-002873 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews records of repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. | [Section 3.1.2](#_3.1.2_Controlled_Maintenance)[Enclosure 4](#_ENCLOSURE_4_–) |
| MA-2 | MA-2 (a) | CCI-002869 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews records of maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. | [Section 3.1.2](#_3.1.2_Controlled_Maintenance)[Enclosure 4](#_ENCLOSURE_4_–) |
| MA-2 | MA-2 (a) | CCI-002871 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the record of repair procedures followed to ensure the organization being inspected/assessed performs repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. | [Section 3.1.2](#_3.1.2_Controlled_Maintenance)[Enclosure 4](#_ENCLOSURE_4_–) |
| MA-2 | MA-2 (a) | CCI-002867 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the record of maintenance procedures followed to ensure the organization being inspected/assessed performs maintenance on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. | [Section 3.1.2](#_3.1.2_Controlled_Maintenance)[Enclosure 4](#_ENCLOSURE_4_–) |
| MA-2 | MA-2 (b) | CCI-000859 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines records of all approvals and monitoring activities to ensure the organization being inspected/assessed approves and monitors all maintenance activities whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. | [Enclosure 4](#_ENCLOSURE_4_–) |
| MA-2 | MA-2 (c ) | CCI-002874 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles who can explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level. | [Section 2.3](#_2.3_Roles_and) |
| MA-2 | MA-2 (c) | CCI-000860 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines: 1. the organization's risk management strategy to ensure the personnel or roles defined in MA-2, CCI 2874 have been designated to approve the removal of the information system or system components;2. and written records of approval for the removal of the information system or system components from organizational facilities for off-site maintenance or repairs to ensure the removal is explicitly approved. | [Section 2.3](#_2.3_Roles_and) |
| MA-2 | MA-2 (d) | CCI-000861 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines written records of media sanitization to ensure the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs. | [Section 4.6](#_4.6_Sanitization) |
| MA-2 | MA-2 (e) | CCI-000862 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines documented evidence of the verification of security controls following maintenance and repair actions to ensure that the organization being inspected/assessed checks all potentially impacted security controls to verify that they are still functioning properly. | [Section 3.3](#_3.3_Verification_of) |
| MA-2 | MA-2 (f) | CCI-002876 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented maintenance-related information to ensure the organization being inspected/assessed defines the maintenance-related information to include in organizational maintenance records. DoD has determined the maintenance-related information is not appropriate to define at the Enterprise level. | [Enclosure 4](#_ENCLOSURE_4_–) |
| MA-2 | MA-2 (f) | CCI-002875 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines maintenance records to ensure they include maintenance-related information defined in MA-2, CCI 2876. | [Enclosure 4](#_ENCLOSURE_4_–) |
| MA-3 | MA-3 | CCI-000865 |  | HighModerateLow |  | The organization conducting the inspection/assessment:1. obtains and examines the Security Plan to ensure the list of approved maintenance tools is documented;2. ensures only the approved maintenance tools are used within the system. | [Section 3.2](#_3.2_Maintenance_Tools) |
| MA-3 | MA-3 | CCI-000866 |  | HighModerateLow |  | The organization conducting the inspection/assessment:1. obtains and examines the Security Plan to identify the list of approved maintenance tools;2. ensures the organization being inspected/assessed controls the approved information system maintenance tools. | [Section 3.2](#_3.2_Maintenance_Tools) |
| MA-3 | MA-3 | CCI-000867 |  | HighModerateLow |  | The organization conducting the inspection/assessment obtains and examines:1. the Security Plan to identify the list of approved maintenance tools; and2. documented procedures to identify how the use of maintenance tools is monitored; and3. reviews evidence that the monitoring is conducted IAW the documented procedures. | [Section 3.2](#_3.2_Maintenance_Tools) |
| MA-3 (1) | MA-3 (1) | CCI-000869 |  | HighModerate |  | The organization conducting the inspection/assessment obtains and examines procedures for, and records of inspection of the maintenance tools carried into a facility by maintenance personnel to ensure the tools are inspected for improper or unauthorized modifications. | [Section 3.2](#_3.2_Maintenance_Tools) |
| MA-3 (2) | MA-3 (2) | CCI-000870 |  | HighModerateLow |  | The organization conducting the inspection/assessment obtains and examines the procedures for checking all diagnostic and test media for malicious code, and a sampling of configuration files and audit logs of the tool set used to check media. The purpose of the review is to ensure the organization being inspected/assessed checks all media containing diagnostic and test programs for malicious code before the media are used in the information system. | [Section 3.2](#_3.2_Maintenance_Tools) |
| MA-3 (3) | MA-3 (3) (a) | CCI-000871 | HighModerateLow |  |  | The organization conducting the inspection/assessment obtains and examines the documented process and record of maintenance equipment removal to ensure the organization being inspected/assessed takes one of the four actions listed in the implementation guidance. | [Enclosure 4](#_ENCLOSURE_4_–) |
| MA-3 (3) | MA-3 (3) (d) | CCI-002882 | HighModerateLow |  |  | The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being inspected/assessed defines the personnel or roles who can provide an exemption that explicitly authorizes removal of equipment from the facility. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level. | [Section 2.3](#_2.3_Role-Based_Training) |
| MA-3 (4) | MA-3 (4) | CCI-002883 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to restrict the use of maintenance tools to authorized personnel only. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2883. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-4 (1) | MA-4 (1) (a) | CCI-002885 |  | HighModerate |  | The organization conducting the inspection/assessment obtains and examines the documented audit events to ensure the organization being inspected/assessed defines the nonlocal maintenance and diagnostic session audit events to audit. DoD has determined the audit events are not appropriate to define at the Enterprise level. | [Section 4.1](#_4.1_Audit) |
| MA-4 (1) | MA-4 (1) (a) | CCI-002884 |  | HighModerate |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to audit nonlocal maintenance and diagnostic sessions' organization-defined audit events. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2884. | [Section 4.1](#_4.1_Audit) |
| MA-4 (1) | MA-4 (1) (b) | CCI-002886 |  | HighModerate |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure the organization being inspected/assessed reviews the records of the nonlocal maintenance and diagnostic sessions. | [Section 4](#_4.0_NONLOCAL_MAINTENANCE)[Enclosure 4](#_ENCLOSURE_4_–) |
| MA-4 (2) | MA-4 (2) | CCI-000881 |  | HighModerate |  | The organization conducting the inspection/assessment obtains and examines the Security Plan to ensure the plan identifies the establishment and use of non-local maintenance and diagnostic connections. | [Section 4](#_4.0_NONLOCAL_MAINTENANCE) |
| MA-4 (3) | MA-4 (3) (a) | CCI-000882 | HighModerateLow | HighModerateLow |  | The organization conducting the inspection/assessment obtains and examines contracts and/or service level agreements for all non-local maintenance and diagnostic services to ensure that any IS used for those services is required to have security level at least as high as the security level implemented on the IS being serviced.  Alternatively, the organization conducting the inspection/assessment ensures the organization being inspected/assessed complies with MA-4 (3) CCIs 883 and 1631. | External Link |
| MA-4 (3) | MA-4 (3) (b) | CCI-000883 | HighModerateLow | HighModerateLow |  | The organization conducting the inspection/assessment obtains and examines maintenance procedures for all non-local maintenance and diagnostic services to ensure that the organization being inspected/assessed sanitizes components before removal from organizational facilities.  Alternatively, the organization conducting the inspection/assessment ensures the organization being inspected/assessed complies with MA-4 (3) CCI 882. | [Section 4.6](#_4.6_Sanitization) |
| MA-4 (3) | MA-4 (3) (b) | CCI-001631 | HighModerateLow | HighModerateLow |  | The organization conducting the inspection/assessment obtains and examines maintenance procedures for all non-local maintenance and diagnostic services to ensure that the organization being inspected/assessed sanitizes and inspects serviced components prior to reusing them on any information system. Alternatively, the organization conducting the inspection/assessment ensures the organization being inspected/assessed complies with MA-4 (3) CCI 882. | [Section 3.4](#_3.4_Sanitization)[Section 4.6](#_4.6_Sanitization) |
| MA-4 (4) | MA-4 (4) (a) | CCI-002887 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented authenticators to ensure the organization being inspected/assessed defines the authenticators that are replay resistant which will be employed to protect nonlocal maintenance sessions. DoD has determined the authenticators are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-4 (4) | MA-4 (4) (a) | CCI-000884 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect nonlocal maintenance sessions by employing authenticators defined in MA-4 (4), CCI 2887 that are replay resistant. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 884. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-4 (4) | MA-4 (4) (b) | CCI-001632 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to protect nonlocal maintenance sessions by separating the maintenance session from other network sessions with the information system by either physically separated communications paths or logically separated communications paths based upon encryption. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 1632. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-4 (5) | MA-4 (5) (a) | CCI-000887 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the maintenance procedures and historical approvals to ensure that the ISSO approves the non-local maintenance. DoD has defined the personnel or roles as the ISSO. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-4 (5) | MA-4 (5) (a) | CCI-0028888 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the ISSO. | Automatically compliant with this CCI because they are covered at the DoD level |
| MA-4 (5) | MA-4 (5) (b) | CCI-002889 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed notifies the user base which could be impacted by the maintenance event of the date and time of planned nonlocal maintenance. DoD has defined the personnel or roles as the user base which could be impacted by the maintenance event. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-4 (5) | MA-4 (5) (b) | CCI-000886 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as the user base which could be impacted by the maintenance event. | Automatically compliant with this CCI because they are covered at the DoD level |
| MA-4 (6) | MA-4 (6) | CCI-002890 | HighModerateLow | HighModerateLow |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2890. | [Section 4.5](#_4.5_Connectivity) |
| MA-4 (6) | MA-4 (6) | CCI-003123 | HighModerateLow | HighModerateLow |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 3123. | Tier-4 |
| MA-4 (7) | MA-4 (7) | CCI-002891 |  | HighModerateLow |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to implement remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2891. | [Section 4.5](#_4.5_Connectivity) |
| MA-4 | MA-4 (a) | CCI-000873 |  | HighModerateLow |  | The organization conducting the inspection/assessment obtains and examines:1. the Security Plan to ensure the procedures for approving non-local maintenance and diagnostic activities are documented; and2. records approving non-local maintenance and diagnostic activities. | [Enclosure 2](#_ENCLOSURE_2_–_1) |
| MA-4 | MA-4 (a) | CCI-000874 |  | HighModerateLow |  | The organization conducting the inspection/assessment obtains and examines:1. the Security Plan to identify the authorized non-local maintenance and diagnostic activities; and2. documented procedures to identify how the use of non-local maintenance and diagnostic activities are monitored; and3. reviews evidence that the monitoring is conducted IAW the documented procedures. | [Section 4](#_4.0_SANITIZATION)[Enclosure 2](#_ENCLOSURE_2_–_1) |
| MA-4 | MA-4 (b) | CCI-000876 |  | HighModerateLow |  | The organization conducting the inspection/assessment obtains and examines:1. the Security Plan to ensure non-local maintenance and diagnostic tools have been identified; and 2. maintenance records to ensure only those tools allowed are used IAW MA-4, CCI 873. | [Section 4](#_4.0_SANITIZATION)[Enclosure 2](#_ENCLOSURE_2_–_1) |
| MA-4 | MA-4 (c) | CCI-000877 |  | HighModerateLow |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions. For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 877. | [Section 4.2](#_4.2_Authentication) |
| MA-4 | MA-4 (d) | CCI-000878 |  | HighModerateLow |  | The organization conducting the inspection/assessment obtains records of authorized non-local maintenance and diagnostic activities, and examines a sampling to verify the organization is maintaining records for all non-local maintenance and diagnostic activities. | [Enclosure 2](#_ENCLOSURE_2_–_1)[Enclosure 4](#_ENCLOSURE_4_–) |
| MA-4 | MA-4 (e) | CCI-000879 |  | HighModerateLow |  | The organization conducting the inspection/assessment obtains and examines audit logs of session and network connections termination for non-local maintenance to ensure session and network connections are terminated when non-local maintenance is completed. | [Section 4.1](#_4.1_Audit)[Section 4.5](#_4.5_Connectivity) |
| MA-5 (1) | MA-5 (1) (a) | CCI-000893 | High | High | High | The organization conducting the inspection/assessment obtains and examines the procedures identified in MA-5, CCI 890 to ensure it includes specific procedures for maintenance personnel that lack appropriate security clearances or are not U.S. citizens. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MA-5 (1) | MA-5 (1) (a) (1) | CCI-000894 | High | High | High | The organization conducting the inspection/assessment obtains and examines the records of maintenance personnel who access the system to ensure the organization being inspected/assessed requires maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals to be escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MA-5 (1) | MA-5 (1) (a) (2) | CCI-000895 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed sanitizes, removes, or physically disconnects all nonvolatile storage media from the system prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MA-5 (1) | MA-5 (1) (b) | CCI-002892 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MA-5 (2) | MA-5 (2) | CCI-000897 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for all compartments of information on the system. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-5 (3) | MA-5 (3) | CCI-000898 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are U.S. citizens. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-5 (4) | MA-5 (4) (a) | CCI-000899 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures that cleared foreign nationals (i.e., foreign nationals with appropriate security clearances), are used to conduct maintenance and diagnostic activities on classified information systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-5 (4) | MA-5 (4) (b) | CCI-000900 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures that approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified information systems are fully documented within Memorandum of Agreements. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-5 (5) | MA-5 (5) | CCI-002893 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures that non-escorted personnel performing maintenance activities not directly associated with the information system but in the physical proximity of the system, have required access authorization. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-5 | MA-5 (a) | CCI-000890 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines procedures addressing maintenance personnel to ensure that the organization being inspected/assessed has established processes for the authorization of maintenance personnel. | [Enclosure 1](#_Enclosure_1_–)[Enclosure 2](#_ENCLOSURE_2_–_1) |
| MA-5 | MA-5 (a) | CCI-000891 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the current list of authorized maintenance organizations or personnel to ensure the organization being inspected/assessed is maintaining the list. | [Enclosure 1](#_Enclosure_1_–)[Enclosure 2](#_ENCLOSURE_2_–_1) |
| MA-5 | MA-5 (b) | CCI-002894 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of personnel performing maintenance on the information system to ensure the organization being inspected/assessed ensures that non-escorted personnel performing maintenance on the information system have required access authorizations. | [Enclosure 4](#_ENCLOSURE_4_–) |
| MA-5 | MA-5 (c ) | CCI-002895 | HighModerateLow | HighModerateLow | HighModerateLow | The organization conducting the inspection/assessment obtains and examines documented organizational personnel to ensure the organization being inspected/assessed designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. | [Enclosure 4](#_ENCLOSURE_4_–) |
| MA-6 | MA-6 | CCI-000903 |  |  | HighModerate | The organization conducting the inspection/assessment obtains evidence that maintenance support is available for information system components defined in MA-6, CCI 2896 and that the support will be provided within 24 hours (Low and Moderate Availability) or immediately upon failure for (High Availability).  Evidence can include maintenance support contracts, inventories of spare parts, etc. DoD has defined the time period as within 24 hours (Low and Moderate Availability) or immediately upon failure for (High Availability).  | [Section 5](#_5.0_SPARES_AND) |
| MA-6 | MA-6 | CCI-002896 |  |  | HighModerate | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components for which it obtains maintenance support and/or spare parts. DoD has determined the information system components are not appropriate to define at the Enterprise level. | [Section 5](#_5.0_SPARES_AND) |
| MA-6 | MA-6 | CCI-002897 |  |  | HighModerate | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the time period as within 24 hours (Low and Moderate Availability) or immediately upon failure for (High Availability). | Automatically compliant with this CCI because they are covered at the DoD level |
| MA-6 (1) | MA-6 (1) | CCI-002898 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines schedules and records of preventive maintenance to ensure the organization being inspected/assessed performs preventive maintenance on information system components defined in MA-6 (1), CCI 2899 at time intervals defined in MA-6 (1), CCI 2900. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-6 (1) | MA-6 (1) | CCI-002899 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines information system components on which to perform preventive maintenance. DoD has determined the information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-6 (1) | MA-6 (1) | CCI-002900 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented time intervals to ensure the organization being inspected/assessed defines time intervals to perform preventive maintenance on organization-defined information system components.  DoD has determined the time intervals are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-6 (2) | MA-6 (2) | CCI-002901 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines schedules and records of predictive maintenance to ensure the organization being inspected/assessed performs predictive maintenance on information system components defined in MA-6 (2), CCI 2902 at time intervals defined in MA-6 (2), CCI 2903. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-6 (2) | MA-6 (2) | CCI-002902 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines information system components on which to perform predictive maintenance. DoD has determined the information system components are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-6 (2) | MA-6 (2) | CCI-002903 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented time intervals to ensure the organization being inspected/assessed defines time intervals to perform predictive maintenance on organization-defined information system components.  DoD has determined the time intervals are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MA-6 (3) | MA-6 (3) | CCI-002904 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documentation of automated mechanisms to ensure the organization being inspected/assessed employs automated mechanisms to transfer predictive maintenance data to a computerized maintenance management system. | NIST has not allocated this AP. Therefore, this AP is not applicable. |

# **ENCLOSURE 1 – AUTHORIZED MAINTENANCE PERSONNEL**

|  |
| --- |
| AUTHORIZED MAINTENANCE PERSONNEL |
| Name | **Company** | **Title** | **Contact Information** | **Authorized Systems** |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# **ENCLOSURE 2 – AUTHORIZED THIRD PARTY MAINTENANCE PERSONNEL**

|  |
| --- |
| AUTHORIZED THIRD PARTY MAINTENANCE PERSONNEL |
| Name | **Company** | **Title** | **Contact Information** | **Authorized Systems** |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# **ENCLOSURE 3 – MAINTENANCE SUPPORT FOR SYSTEM COMPONENTS**

|  |
| --- |
| {ACRONYM} |
| Component Name | **Spare Asset** | **Support Contract** | **24 Hour Availability** |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |
|  |  | Choose an item. | Choose an item. |

# **ENCLOSURE 4 – MAINTENANCE LOG**

|  |
| --- |
| {ACRONYM} MAINTENANCE LOG |
| Date | **Individual Performing Maintenance** | **Name of Escort (if required)** | **Description of Maintenance** | **Affected Equipment** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |