Redacted

INFORMATION SYSTEM CONTINUOUS MONITORING (ISCM) PLAN

Redacted

Version:
1.0
Date:
20220901

EXECUTIVE SUMMARY

The Continuous Monitoring Plan is designed to ensure that [redacted] effectively maintains the [redacted] information system security and compliance posture. [redacted] will ensure continuous management of system security documentation, POA&Ms, vulnerabilities, and change control requests. [redacted] must implement a process to plan, schedule, and conduct penetration testing by an independent assessor as required to ensure compliance to the vulnerability management program. Annual updates and reviews are critical in maintaining the relevance and effectiveness of this plan.

[redacted]

REPARED BY

Identification of Organization that Prepared this Document		
[redacted]	Organization Name	[redacted]
	Street Address	
	Suite/Room/Building	
	City, State Zip	

Prepared for

Identification of Cloud Service Provider		
[redacted]	Organization Name	[redacted]
	Street Address	
	Suite/Room/Building	
	City, State Zip	

Template Revision History

Date	Description
9/1/2022	Original publication

Document Revision History

Date	Description	Version of CMP	Author

How to contact us

For technical questions about this document contac[redacted]

TABLE OF CONTENTS

1. INTRODUCTION 1

1.1 SCOPE 1

1.2 ROLES & RESPONSIBILITIES 1

1.3 CHANGES AND REVISIONS 1

2. CONTINUOUS MONITORING REQUIREMENTS 1

3. SECURITY ASSESSMENTS & AUTHORIZATIONS 1

3.1 ASSESSMENTS 1

3.2 AUTHORIZATIONS........ 2

3.3 SYSTEM INTERCONNECTIONS 2

4. DOCUMENTATION 3

4.1 SYSTEM SECURITY PLAN, SECURITY POLICIES, AND SUPPORTING PLANS 3

4.2 RULES OF BEHAVIOR AND ACCESS AGREEMENTS 3

5. CONTINUOUS MONITORING PROCEDURE 3

5.1 SECURITY REASSESSMENT........ 3

5.2 SECURITY DOCUMENTATION REVIEWS AND UPDATES 3

5.3 PROCEDURAL TESTING........ 4

5.4 VULNERABILITY SCANNING, FLAW REMEDIATION, AND SYSTEM INTEGRITY MONITORING...... 4

5.5 PLAN OF ACTION AND MILESTONES (POA&M) MANAGEMENT AND SUBMISSION 4

6. COMPLIANCE 5

7. STATERAMP SUPPORTING DOCUMENTATION MANAGEMENT 5

7.1 VULNERABILITY SCANNING........ 6

7.2 STATERAMP CONTINUOUS MONITORING AND POA&M DOCUMENT MANAGEMENT 7

1. INTRODUCTION

1.1 SCOPE

This Information System Continuous Monitoring (ISCM) Plan applies to all employees, to include contract personnel. As directed, key personnel will be appointed to perform duties in support of the ISCM. All devices and data within [redacted] boundary, as documented in the system authorization, fall under the requirements of this plan. Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, up to and including termination of employment.

1.2 ROLES & RESPONSIBILITIES

The following individual(s) or group(s) are responsible for developing, implementing, coordinating, complying with, and maintaining the Continuous Monitoring Plan and its associated mechanisms:

ROLE	CONTINUOUS MONITORING RESPONSIBILITY
President	Oversight and management of the continuous monitoring process.
Systems Administrator	Development of continuous monitoring artifacts and reporting.

1.3 CHANGES AND REVISIONS

The ISCM Plan is to be reviewed and updated by [redacted] Information Security Manager at least annually. Changes or revisions to this policy must be communicated to [redacted] personnel with access to the [redacted] information system as changes or revisions are made. Employees within [redacted] must acknowledge and comply with changes to the policy.

2. CONTINUOUS MONITORING REQUIREMENTS

The [redacted] ISCM Plan ensures that every control is monitored for effectiveness, and every control is subject to use in monitoring security status. Data sources include people, processes, technologies, the computing environment, as well as any existing relevant security control assessment reports. The following continuous monitoring requirements, mechanisms, and provisions are to be applied for all employees, management, contractors, and other users who operate within the [redacted] information system boundary.

3. SECURITY ASSESSMENTS & AUTHORIZATIONS

3.1 ASSESSMENTS

[redacted] will develop and implement a Security Assessment Plan that includes the scope of the entire [redacted] information system [redacted] may employ an independent penetration agent or penetration team to perform penetration testing on the [redacted] information system.

3.2 AUTHORIZATIONS

[redacted] will update the security authorization at least every three years or when a significant change occurs that affects the system or operating environment.

3.3 SYSTEM INTERCONNECTIONS

[redacted] must authorize all direct connections with other information systems using Interconnection Security Agreements (ISAs) that document the security requirements and nature of information communicated between the two systems. All agreements must be reviewed every three years unless there is a significant change in the interaction between the systems in which it would be updated at that time. At this [redacted] does not use interconnected systems.

[redacted] must receive any security-related audit reports available from the interconnected to system to include, if applicable, SOC1, SOC2, ATO Package or other reports of attestation.

[redacted] must prohibit the direct connection of any system to an external network without the use of a cryptographic information protections.

4. DOCUMENTATION

4.1 SYSTEM SECURITY PLAN, SECURITY POLICIES, AND SUPPORTING PLANS

[redacted] has developed a System Security Plan (SSP) for the [redacted] that provides an overview of the system and its function, describes the security controls that are in place, planned, or partially implemented, and provides details of how the controls are implemented. The security controls selection and implementation is consistent with the requirements of NIST SP 800-53 Revision 4. The [redacted] SSP must be consistent with the security architecture, explicitly define the authorization boundary for the system, describe the operational context of the information system, provide an overview of the security requirements of the system, and describe in detail how each applicable security control is implemented.

The [redacted] SSP, security policies, and security plans must be protected from unauthorized modifications and in accordance with internal policies that define sensitive information storage.

4.2 RULES OF BEHAVIOR AND ACCESS AGREEMENTS

[redacted] must establish and document guidance that governs the acceptable use of information and information systems. These documented rules and behavior requirements must be readily available to all employees. Before authorizing any access to information and the information system, [redacted] must receive a signed acknowledgement from all employees.

In the rules of behavior, [redacted] must include explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

5. CONTINUOUS MONITORING PROCEDURE

5.1 SECURITY REASSESSMENT

In addition to all applicable security controls in this baseline being assessed prior to authorization, an independent security assessment must be performed every 5 years or as needed to include:

- All critical security controls as identified in the Continuous Monitoring Strategy Guide
- One third of the remaining security controls
- All security controls related to any remediated items in the previous 12 months
- All other assessments required per the Continuous Monitoring Strategy Guide to include an external Penetration Test

5.2 SECURITY DOCUMENTATION REVIEWS AND UPDATES

[redacted] must be reviewed and updated annually, or when there are significant changes to the information system or if the control implementation details have changed due to results of an internal or external security assessment.

In addition, [redacted] conducts annual updates and reviews of all policies and plans to maintain relevance and efficiency.

[redacted] must review and update the rules of behavior annually or when there are significant changes. [redacted] must require individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised /updated.

5.3 PROCEDURAL TESTING

[redacted] operationally tests the procedures contained in the Incident Response Plan (IRP) and the Information System Contingency Plan (ISCP) to ensure the plans will function appropriately in the event of a real-life scenario. [redacted] must test and exercise the ISCP using functional exercises on an annual basis. In addition, a new ISCP Test Report must be inserted into the proper Appendix of the ISCP.

[redacted] must conduct annual security incident response testing. Upon the completion of the System Security Plan update, [redacted] must record the results of the incident response testing directly in the SSP control description box indicating when testing took place, testing materials, who participated, and who conducted the testing.

5.4 VULNERABILITY SCANNING, FLAW REMEDIATION, AND SYSTEM INTEGRITY MONITORING

[redacted] must scan all operating systems, web applications, and databases with admin credentials within the system environment on a monthly basis. Before each scan, [redacted] must update the list of vulnerabilities scanned on a continuous basis. [redacted] will mitigate all discovered high-risk vulnerabilities within 30 days, all moderate-risk vulnerabilities within 90 days, and all low-risk vulnerabilities within 180 days. Due to the sensitivity of the mitigation evidence, these vulnerability scan artifacts and reports are retained [redacted] and are uploaded to the PMO repository.

Upon the release of updates, [redacted] install security-relevant software and firmware updates within 30 days. [redacted] must also perform integrity scans on a monthly basis to ensure that all patching and flaw remediation updates are conducted in an authorized manner.

Vulnerabilities that are identified with vulnerability scanning and cannot be immediately remediated are categorized and documented on the POA&M, in accordance with Section 2.7 below.

5.5 PLAN OF ACTION AND MILESTONES (POA&M) MANAGEMENT AND SUBMISSION

The Plan of Action and Milestones (POA&M) document serves as a high-level work plan to correct audit findings in [redacted] security implementation. The POA&M identifies and lists audit findings discovered through independent annual 3PAO security assessments and the monthly vulnerability scans described above. [redacted] stores the latest POA&M internally, accessible only [redacted] personnel.

StateRAMP requires [redacted] to formally update and communicate POA&M status on a monthly basis. An updated POA&M will be submitted monthly to the sponsoring agency. In addition to the updated POA&M submission, [redacted] will also send the sponsoring agency updated vulnerability scan artifacts and reports to show evidence that outstanding high-risk and applicable moderate-risk vulnerabilities have been mitigated. The sponsoring agency reviews POA&M status for unacceptable risk exposure. Inappropriately managed POA&M items or elevated risk posture presented by new vulnerabilities are communicated to the sponsoring agency CIO as necessary.

6. COMPLIANCE

All [redacted] employees are required to comply with the continuous monitoring requirements above. In addition to individual disciplinary actions, failure to comply could results in the revocation of [redacted] authority to operate.

7. STATERAMP SUPPORTING DOCUMENTATION MANAGEMENT

The following documentation tasks must be performed on a regular basis in order to maintain StateRAMP compliance.

Task	Task Description
1.1	Prior to any annual StateRAMP assessment processes, initiate a review of the StateRAMP control narratives present in the SSP, information system policies, and StateRAMP supporting documents and identify if there is any control narrative change in [redacted] environment. If there is a change, identify scope of the change, whether the change can be updated in the control narrative or needs additional discussion with the control owners.
1.2	For those controls within the StateRAMP baseline where the control narrative has not changed, update review status to indicate the control narrative has been reviewed for accuracy and completeness and there are no changes required prior to annual assessment
1.3	For those controls within the StateRAMP baseline where the control narrative has changed, update the control narrative in the SSP, information system policies and StateRAMP supporting documentation for all the controls affected by the control change in the [redacted]} environment. For all control implementation changes that require information gathering sessions prior to documentation, control owners will conduct meetings to analyze the scope and impact of change to the StateRAMP status. Control owners will gather information from the meetings to update the control narrative for those changes to the StateRAMP status.
1.4	For those controls within the StateRAMP baseline where the control narrative has changed, update review status to indicate the control narrative has been reviewed for accuracy and completeness and that all required changes have been completed prior to annual assessment.
1.5	Review and update the current security policies for [redacted] system for federal customers every 3 years or when required due to changes in the environment.
1.6	Review and update the current procedures related to the security of the [redacted] system for federal customers annually or when required due to changes in the environment.
1.7	Review and update Interconnection Security Agreements (ISAs) between [redacted] system and any connected third-party systems every 3 years or when there is a significant change in the interaction between the systems.
1.8	Review and update the current Incident Response Plan (IRP) for the [redacted] system for federal customers annually or when required due to changes in the environment.
1.9	Review and update the current Information System Contingency Plan (ISCP) for [redacted] system for federal customers annually or when required due to changes in the environment.

Task	Task Description
1.10	Review and update the current Configuration Management Plan (CMP) for the [redacted] for federal customers annually or when required due to changes in the environment.

Table 1. StateRAMP Supporting Documentation Management – Annually

7.1 VULNERABILITY SCANNING

The following vulnerability scanning tasks must be performed on a regular basis in order to maintain StateRAMP compliance.

Task	Task Description	Responsible Roles
2.1	Generate list of [redacted] system components (servers, web applications, and databases) from the hardware and software inventory on a monthly basis and upload to the PMO repository.	System Administrator
2.2	Execute monthly vulnerability and patch management scan reports for in-scope information system components	System Administrator
2.3	Review vulnerability scan results in order to determine next steps for all vulnerabilities, including actionable vulnerabilities, zero-day vulnerabilities, and excluded vulnerabilities. All vulnerabilities will be tracked and documented using the procedures described in Table 3 “Vulnerability Tracking and Remediation” below.	System Administrator
2.4	Upload original monthly vulnerability scan results to the PMO document repository, corresponding to the monthly continuous monitoring status report.	System Administrator

Table 2. Vulnerability Scanning and Analysis – Monthly

Task	Task Description	Responsible Roles
3.1	Import actionable vulnerabilities and zero-day vulnerabilities into tickets and [redacted] POA&M document (refer to Table 4, Documenting New POA&M Items, for more information)	System Administrator
3.2	Import excluded vulnerabilities into the corresponding worksheet within [redacted] POA&M document (refer to Table 4, Documenting New POA&M Items, for more information) and ensure there is a business or risk acceptance rationale completed for each exclusion.	System Administrator
3.3	Remediate identified zero-day vulnerabilities immediately (for StateRAMP as soon as feasible).	System Administrator
3.4	Monitor status of identified actionable vulnerabilities in accordance with StateRAMP timelines for high risk (30 days) and moderate risk (90 days) vulnerabilities, using tickets and the POA&M document.	System Administrator
3.5	Remediate identified actionable vulnerabilities for StateRAMP in accordance with StateRAMP timelines for high risk (30 days) and moderate risk (90 days) vulnerabilities.	System Administrator
3.6	For closed actionable and zero-day vulnerabilities, pull targeted vulnerability scan results from the vulnerability scanning tool to demonstrate corresponding patch or vulnerability fix has been applied and vulnerability no longer shows on scan report and is not present within the [redacted] system.	System Administrator

TASK	TASK DESCRIPTION	RESPONSIBLE ROLES
3.7	Upload monthly vulnerability scan results to the PMO document repository, corresponding to the monthly continuous monitoring status report.	System Administrator
3.8	For closed actionable and zero-day vulnerabilities that no longer show on vulnerability scan reports, close associated ticket [redacted] POA&M item once remediation is complete.	System Administrator

Table 3. Vulnerability Tracking and Remediation – Monthly

7.2 STATERAMP CONTINUOUS MONITORING AND POA&M DOCUMENT MANAGEMENT

The following POA&M management tasks must be performed on a regular basis in order to maintain StateRAMP compliance.

TASK	TASK DESCRIPTION	RESPONSIBLE ROLES
4.1	On an annual basis, for each risk finding of the annual security assessment, create a new actionable POA&M item within the POA&M and input following data: POA&M item (risk finding) description, [redacted] point of contact, POA&M item status, POA&M item original risk rating, POA&M item adjusted risk rating and rationale for adjusted risk rating. Create a corresponding ticket to assist with POA&M item tracking.	System Administrator
4.2	In accordance with Table 3, Vulnerability Tracking and Remediation, import actionable vulnerabilities and zero-day vulnerabilities available for StateRAMP tracking into tickets and the POA&M. Within the POA&M, create a new actionable POA&M item within the POA&M and input the following data: POA&M item (risk finding) description, [redacted] point of contact, POA&M item status, POA&M item original risk rating, POA&M item adjusted risk rating and rationale for adjusted risk rating	System Administrator
4.3	In accordance with Table 3, Vulnerability Tracking and Remediation, import excluded vulnerabilities and accompanying business or risk acceptance rationale into the corresponding worksheet within the POA&M document. Input the following data: POA&M item (risk finding) description, [redacted] of contact, POA&M item status of exclusion, and the business or risk acceptance rationale for POA&M item exclusion	System Administrator
4.4	Review all actionable POA&M items, including all risk findings and all actionable and zero-day vulnerabilities to determine potential [redacted] response: Remediation of POA&M item within corresponding StateRAMP timelines – as soon as possible for zero-day actionable POA&M items 30 days for high-risk actionable POA&M items, 90 days for moderate-risk actionable POA&M items (no deviation), Extension of corresponding remediation timeline for POA&M item (deviation), or risk acceptance of POA&M item (deviation).	System Administrator
4.5	For actionable POA&M items where [redacted] to deviate from StateRAMP timelines or risk acceptance guidelines, [redacted] document the following in a way that can be easily reported in accordance with StateRAMP POA&M item deviation requirements: POA&M item remediation milestone changes, Business / operational requirements for POA&M item milestone changes, Extensions for	System Administrator

TASK	TASK DESCRIPTION	RESPONSIBLE ROLES
	POA&M item milestone completion dates, POA&M item risk reduction rationale, POA&M item risk acceptance rationale.	
4.6	Following review and documentation of any deviations, update all actionable POA&M items with any changes to: POA&M item scheduled completion date, POA&M item remediation milestones, POA&M item risk ratings, and any POA&M item risk adjustment rationale	System Administrator

Table 4. Documenting New POA&M Items – Monthly

TASK	TASK DESCRIPTION	RESPONSIBLE ROLES
5.1	Monitor status of remediation milestones, completion, issues, and risks for all actionable POA&M items (new and previously identified) using the corresponding ticket and the [redacted] POA&M document.	System Administrator
5.2	For all previously identified actionable POA&M items that were identified in prior assessments and exist in the POA&M prior to monthly new POA&M item intake (through other compliance or risk assessment sources, past vulnerability scans, or as internally reported), review for completeness and update if necessary.	System Administrator
5.3	Identify all actionable POA&M items (new and previously identified) that will be remediated during the monthly timeframe, in accordance with StateRAMP remediation timelines: as soon as possible for zero-day actionable POA&M items 30 days for high-risk actionable POA&M items, 90 days for moderate-risk actionable POA&M items. Vulnerability scan related actionable POA&M items are handled in accordance with Table 3, Vulnerability Tracking and Remediation.	System Administrator
5.4	Remediate actionable POA&M items that have been identified during vulnerability scans in accordance with established remediation procedures for that particular class of vulnerability.	System Administrator
5.5	For closed actionable POA&M items, pull targeted evidence artifacts and reports to demonstrate POA&M item remediation has been completed and the POA&M item is not present within the [redacted] information system.	System Administrator
5.6	For closed actionable POA&M items, close corresponding ticket and [redacted] POA&M item once remediation is complete.	System Administrator

Table 5. POA&M Item Tracking and Remediation – Monthly

TASK	TASK DESCRIPTION	RESPONSIBLE ROLES
6.1	In order to meet StateRAMP continuous monitoring requirements, compile the following documents from document repository a week prior to the established monthly continuous monitoring reporting date: • Original vulnerability scan results from the vulnerability scanning tool for the corresponding reporting cycle • Targeted vulnerability scan results as evidence that closed vulnerabilities have been patched prior to the reporting date	System Administrator

TASK	TASK DESCRIPTION	RESPONSIBLE ROLES
	- POA&M document containing all open actionable POA&M items - Within the POA&M document, the POA&M worksheet of excluded vulnerabilities with corresponding business or risk acceptance rationale	
6.2	Develop high-level vulnerability status report using the Continuous Monitoring Monthly Executive Summary template provided on the StateRAMP website, per the Continuous Monitoring Strategy Guide. Provide an overview of the following: - Risk adjustments or false positives for any scan findings - Status of Annual Assessment - Details of POA&M issues if present - Late High Items (note pending deviations) - Late Moderate Items (note pending deviations) - Evidence of remediation of any POA&M findings	System Administrator
6.3	Review original vulnerability scan results, targeted vulnerability scan results, high-level vulnerability status report, high-level POA&M status report, and [redacted] POA&M document for quality assurance; obfuscate sensitive data (IP address ranges, hostnames, etc.) within reports prior to submission.	System Administrator
6.4	Upload original vulnerability scan reports, targeted vulnerability scan results, high-level vulnerability status report, inventory, Continuous Monitoring Monthly Executive Summary, and updated POA&M to the PMO repository.	System Administrator or a member of the Security Control Team

Table 6. StateRAMP Monthly Reporting – Monthly