Continuous Monitoring Strategy & Guide

Version 1.0

June 27, 2012

Executive Summary

The OMB memorandum M-10-15, issued on April 21, 2010, changed from static point in time security authorization processes to Ongoing Assessment and Authorization throughout the system development life cycle. Consistent with this new direction favored by OMB and supported in NIST guidelines, FedRAMP has developed an ongoing assessment and authorization program for the purpose of reauthorizing Cloud Service Providers (CSP) annually.

After a system receives a FedRAMP Provisional Authorization, it is possible that the security posture of the system could change over time due to changes in the hardware or software on the cloud service offering, or also due to the discovery and provocation of new exploits. Ongoing assessment and authorization provides federal agencies using cloud services a method of detecting changes to the security posture of a system for the purpose of making risk-based decisions.

This guide describes the FedRAMP strategy for CSPs to use once they have received a FedRAMP Provisional Authorization. CSPs must continuously monitor their cloud service offering to detect changes in the security posture of the system to enable well-informed risk-based decision making. This guide instructs CSPs on the FedRAMP strategy to continuously monitor their systems.

Document Revision History

Date	Pages and/or Section #s	Description	Author
6/14/2012	All	Version 1.0	FedRAMP Office

Table of Contents

List of Tables

List of Figures

ABOUT THIS DOCUMENT

This document has been developed to provide guidance on continuous monitoring and ongoing authorization in support of maintaining a FedRAMP. This document is not a FedRAMP template -- there is nothing to fill out in this document.

Who should use this document?

This document is intended to be used by Cloud Service Providers (CSPs), Third Party Assessor Organizations (3PAOs), government contractors working on FedRAMP projects, and government employees working on FedRAMP projects. This document may also prove useful for other organizations that are developing their continuous monitoring program.

How this document is organized

This document is divided into seven sections. Most sections include subsections.

Section 1 provides an overview of the continuous monitoring process.

Section 2 describes roles and responsibilities for stakeholders other than CSPs.

Section 3 describes how operational visibility into the CSP security control implementation supports continuous monitoring.

Section 4 describes the change control process.

Section 5 describes security control frequencies.

Section 6 describes self-attestation deliverables.

Section 7 describes an overview of incident response expectations.

Conventions used in this document

This document uses various typographical conventions.

Italic

Italics are used for email addresses, security control assignments parameters, and formal document names.

Italic blue in a box

Italic blue text in a blue box indicates instructions to the individual filling out the template.

Instruction: This is an instruction to the individual filling out of the template.

Bold

Bold text indicates a parameter or an additional requirement.

`Constant width`

Constant width text is used for text that is representative of characters that would show up on a computer screen.

<**Brackets**>

Bold blue text in brackets indicates text that should be replaced with user-defined values. Once the text has been replaced, the brackets should be removed.

Notes

Notes are found between parallel lines and include additional information that may be helpful to the users of this template.

Note: This is a note.

Sans Serif

Sans Serif text is used for tables, table captions, figure captions, and table of contents.

How to contact us

If you have questions about FedRAMP or something in this document, please write to:

info@fedramp.gov

For more information about the FedRAMP project, please see the website at:

http://www.fedramp.gov.

1. OVERVIEW

Within the FedRAMP Concept of Operations (CONOPS), once an authorization has been granted, the CSP's security posture is monitored according to the assessment and authorization process illustrated in Figure 1. Monitoring security controls is part of the overall risk management framework for information security and is a requirement for CSPs to maintain their FedRAMP Provisional Authorization.

Traditionally, this process has been referred to as "Continuous Monitoring" as noted in *NIST SP 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations*. Other NIST documents such as NIST SP 800-37, Revision 1 refer to "ongoing assessment of security controls". It is important to note that both the terms "Continuous Monitoring" and "Ongoing Security Assessments" mean essentially the same thing and should be interpreted as such.

Performing ongoing security assessments determines whether the set of deployed security controls in an information system remains effective in light of new exploits and attacks, and planned and unplanned changes that occur in the system and its environment over time. To receive reauthorization of a FedRAMP Provisional Authorization from year to year, CSPs must monitor their security controls, assess them on a regular basis, and demonstrate that the security posture of their service offering is continuously acceptable.

Ongoing assessment of security controls results in greater transparency into the security posture of the CSP system and enables timely risk-management decisions. Security-related information collected through continuous monitoring is used to make recurring updates to the security assessment package. Ongoing due diligence and review of security controls enables the security authorization package to remain current which allows agencies to make informed risk management decisions as they use cloud services.

2.1 Purpose of This Document

This document is intended to provide CSPs with guidance and instructions on how to implement their continuous monitoring program. Certain deliverables and artifacts related to continuous monitoring that FedRAMP requires from CSP's are discussed in this document. Additionally, CSPs will find this document useful in understanding how to fill out the annual Self-Attestation template required by FedRAMP.

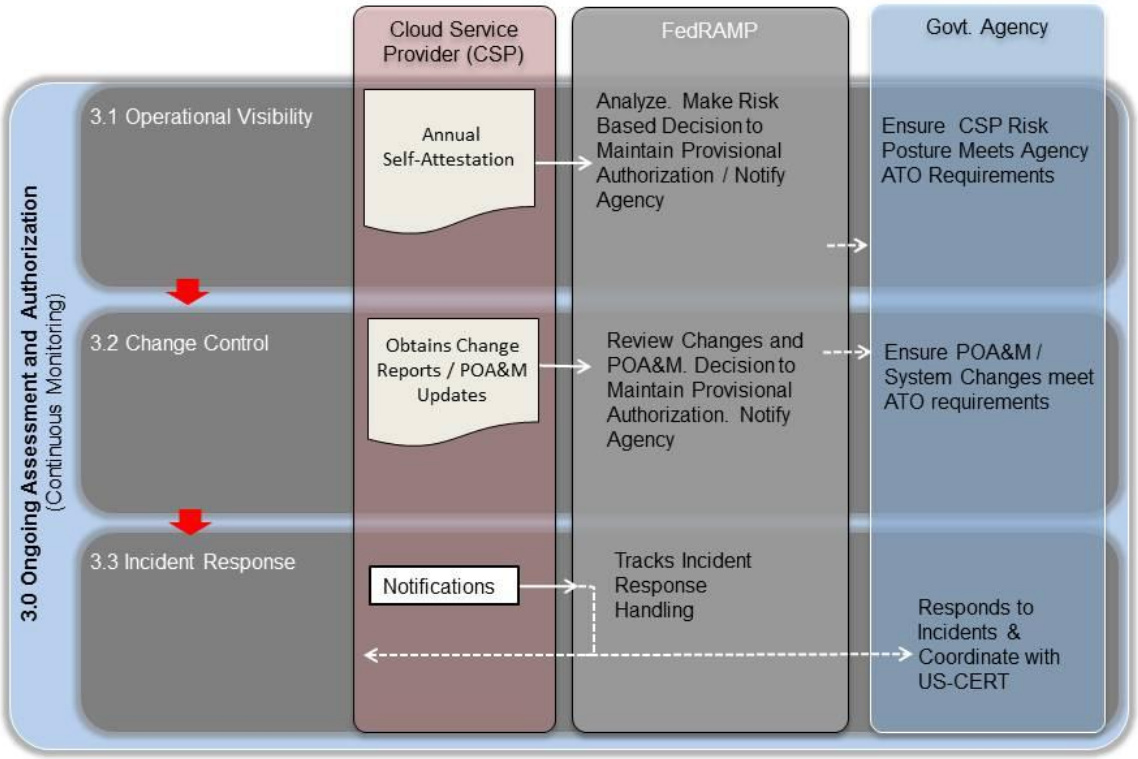

Figure 1. Ongoing Assessment and Authorization Process Areas

2.2 Continuous Monitoring Process

The FedRAMP continuous monitoring program is based on the continuous monitoring process described in *NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organization*. A goal is to provide: (i) operational visibility; (ii) annual self-attestations on security control implementations; (iii) managed change control; (iv) and attendance to incident response duties.

The effectiveness of a CSP's continuous monitoring capability supports ongoing authorization and reauthorization decisions. Security-related information collected during continuous monitoring is used to make updates to the security authorization package. The updated documents provide evidence that FedRAMP baseline security controls continue to safeguard the system as originally planned.

As defined by the National Institute of Standards and Technology (NIST) the process for continuous monitoring includes the following initiatives:

- **Define** a continuous monitoring strategy based on risk tolerance that maintains clear visibility into assets and awareness of vulnerabilities and utilizes up-to-date threat information.

- **Establish** measures, metrics, and status monitoring and control assessments frequencies that make known organizational security status and detect changes to information system infrastructure and environments of operation, and status of security control effectiveness in a manner that supports continued operation within acceptable risk tolerances.
- **Implement** a continuous monitoring program to collect the data required for the defined measures and report on findings; automate collection, analysis and reporting of data where possible.
- **Analyze** the data gathered and **Report** findings accompanied by recommendations. It may become necessary to collect additional information to clarify or supplement existing monitoring data.
- **Respond** to assessment findings by making decisions to either mitigate technical, management and operational vulnerabilities; or accept the risk; or transfer it to another authority.
- **Review** and **Update** the monitoring program, revising the continuous monitoring strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities; further enhance data driven control of the security of an organization's information infrastructure; and increase organizational flexibility.

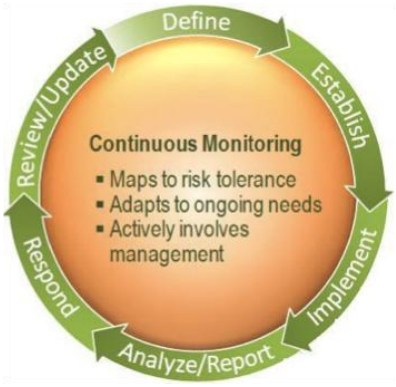

Figure 2. NIST Special Publication 800-137 Continuous Monitoring Process

Security control assessments performed periodically validate whether stated security controls are implemented correctly, operating as intended, and meet FedRAMP baseline security controls. Security status reporting provides federal officials with information necessary to make risk-based decisions and provides assurance to existing customer agencies regarding the security posture of the system.

2. CONTINUOUS MONITORING ROLES & RESPONSIBILITIES

2.1 FedRAMP Office Role

The FedRAMP Program Management Office (PMO) serves as the focal point for coordination of continuous monitoring activities for all stakeholders. Each CSP is assigned an Information

Systems Security Officer (ISSO) by the FedRAMP PMO. CSPs send security control artifacts to their ISSO at various points in time. The ISSOs monitors both the Plan of Action & Milestones (POA&M) and any significant changes and reporting artifacts (such as vulnerability scan reports) associated with the CSP service offering. ISSOs provide the Joint Authorization Board (JAB) with updated information on the system so that risk-based decisions can be made about ongoing authorization.

2.2 DHS Role

The FedRAMP Policy Memo released by OMB defines the DHS FedRAMP responsibilities to include:

- Assisting government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cybersecurity
- Coordinating cybersecurity operations and incident response and providing appropriate assistance
- Developing continuous monitoring standards for ongoing cybersecurity of Federal information systems to include real-time monitoring and continuously verified operating configurations
- Developing guidance on agency implementation of the Trusted Internet Connection (TIC) program with cloud services.

The FedRAMP PMO works with DHS to incorporate their guidance into the FedRAMP program guidance and documents.

2.3 Agency Role

Leveraging agencies should review the artifacts provided through the FedRAMP continuous monitoring process to ensure that the risk posture of the CSP falls within agency tolerance. Additionally, agency customers must perform the following tasks in support of CSP continuous monitoring:

- Provide a POC for CSPs to communicate with
- Notify US-CERT when a CSP reports an incident
- Work with CSPs to resolve incidents by providing coordination with US-CERT
- Notify CSPs if the Agency becomes aware of an incident that a CSP has not yet reported
- Monitor security controls that are agency responsibilities
- Notify ISSOs if a CSP has reported an incident.

During incident response, both CSPs and leveraging agencies are responsible for coordinating incident handling activities together, and with US-CERT. The team based approach to incident handling ensures that all parties are informed and enables incidents to be closed as quickly as possible.

3. OPERATIONAL VISIBILITY

An important aspect of a CSP's continuous monitoring program is to provide evidence that demonstrate the efficacy of their program. At various intervals, evidentiary information is provided to FedRAMP and consuming agencies in the form of artifacts after the FedRAMP Provisional Authorization is granted. The submission of these deliverables and artifacts allows FedRAMP and agency authorizing officials to evaluate the risk posture of the CSP's service offering. Key deliverables are required at the time of annual Self-Attestation. Table 4-1 notes which deliverables are required as part of the annual Self-Attestation and also includes other required continuous monitoring activities. FedRAMP provides a separate Self-Attestation template for CSPs that must be submitted annually one year from the date of the Provisional Authorization and each year therafter.

4. CHANGE CONTROL

Systems are dynamic and FedRAMP anticipates that all systems are in a constant state of change. Configuration management and change control processes help maintain a secure baseline configuration of the CSP's architecture. Routine day-to-day changes are managed through the CSP's change management process described in their *Configuration Management Plan*. However, before a planned significant change takes place, CSP's must perform a Security Impact Analysis to determine if the change will adversely affect the security of the system. The Security Impact Analysis is a standard part of a CSP's change control process as described in the CSP's *Configuration Management Plan*.

CSPs must notify the ISSO of any planned significant changes. The notification of the planned significant change must take place prior to the implementation of the significant change. The ISSO will send the CSP a *Significant Change Security Impact Analysis Form* which will need to be filled out and returned to the ISSO. The planned change will be reviewed by the ISSO and then forwarded to the JAB for approval. All plans for significant changes should include rationale for making the change, and plans for testing the change prior to moving it to the production system.

If any anticipated change either adds residual risk, changes a leveraging agency's security posture, or creates other risk exposure that the JAB finds unacceptable, the Provisional Authorization could be revoked if the change is made without prior approval. A goal is for CSPs to make planned changes in a controlled manner so that the security posture of the system is not decreased.

Within 30 days of significant change occurring, the CSP must submit a new *Security Assessment Report* to the ISSO based on a fresh security assessment performed by a 3PAO. Additionally, the CSP will need to submit an updated security assessment package that contains updated documentation and artifacts pertaining to the newly implemented changes.

FedRAMP will notify leveraging agencies when a significant change is planned, and when a significant change has occurred. Upon notification that a significant change is planned, customer

agencies should inform FedRAMP if they believe the planned changes will adversely affect the security of their information. After an approved change has occurred, customer agencies should review the change artifacts to familiarize themselves with the implementation details.

5. CONTROL FREQUENCIES & SELF-ATTESTATION

Security controls have different frequencies for performance and review, and some controls require review more often than others. Table 4-1 summarizes the frequencies required for the different continuous monitoring activities. Some continuous monitoring activities require that the CSP submits a deliverable to their FedRAMP ISSO. Other continuous monitoring activities do not require a deliverable, and will be reviewed by 3PAOs during security assessments. CSPs must be able to demonstrate to 3PAOs that ongoing continuous monitoring activities are in place, and have been occurring as represented in the *System Security Plan*. For example, if a CSP has indicated in their *System Security Plan* that they monitor unsuccessful login attempts on an ongoing basis, the 3PAO may ask to see log files, along with the CSP analysis of the log files, for random dates over the course of the prior 3-6 months.

In Table 4-1, refer to the Description column for information about what is required and when it is required to be submitted. A checkmark in the 4th column of Table 4-1 indicates that a deliverable is required. In some cases, the deliverable is a component of the annual Self-Attestation.

If an ISSO becomes concerned about the security posture of the CSP system, the ISSO may ask for a security artifact at any point in time. For example, if a CSP indicates in their *System Security Plan* that they actively monitor information system connections, the ISSO could ask the CSP to send them log file snippets for a particular connection at any point in time. If it becomes known that an entity that a CSP has interconnections to has been compromised by an unauthorized user, the ISSO may have legitimate reasons to check in on the interconnection monitoring of the CSP. CSPs should anticipate that aside from annual continuous monitoring deliverables, and aside from testing performed by 3PAOs, that the FedRAMP ISSO may request certain system artifacts on an ad hoc basis if there are concerns.

CSPs are required to attest to the ongoing implementation of their security controls on an annual basis. Certain deliverables are required at the time of the annual Self-Attestation. Deliverables that are required for the annual Self-Attestation are indicated in the Notes column in Table 4-1. These same deliverables are further described in Section 6 of this document. FedRAMP provides a separate Self-Attestation template to help organize these deliverables. Section 6 of this document provides guidance on how to fill out the Self-Attestation template.

When managing continuous monitoring activities, it can be helpful to set up a schedule and an annual information security calendar to plan these activities in advance.

Table 4-1. Summary of Continuous Monitoring Activities & Deliverables

Control Name	Control ID	Description	CSP Authored Deliverable	3PAO Authored Deliverable	Notes
Continuous and Ongoing					
Remote Control	AC-17(5)	CSPs must monitor for unauthorized remote connections continuously and take actions appropriate actions if unauthorized connections are discovered.			
Auditable Events	AU-2d	Certain events must be continuously monitored: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.			
Information System Connections	CA-3c	CSPs must actively monitor information system connections at all times.			Verify the enforcement of security requirements. This control is particularly important for interconnections to other systems and is typically performed on VPNs, switches, routers, firewalls etc..
Information System Component Inventory	CM-8(3)a	CSPs must be able to detect new assets continuously (with a 5 minute delay in detection).			This activity should be automated.
Incident Reporting	IR-6	CSPs should notify customer agencies, and the ISSO, of new incidents as they are discovered. CSPs should fill out Incident Report Forms as needed.	✓		Self-Attestation § 3.1

Control Name	Control ID	Description	CSP Authored Deliverable	3PAO Authored Deliverable	Notes
Temperature & Humidity Controls	PE-14(b)	CSPs must monitor temperature and humidity controls continuously.			Please refer to ASHRAE *Thermal Guidelines for Data Processing Environments*.
Vulnerability Scanning	RA-5(2)	CSPs must update the list of vulnerabilities scanned continuously, before each scan.			This means that before you run a scan, you should update the signatures to use the most current version(s) available.
Weekly					
Audit Review, Analysis, & Reporting	AU-6a	CSPs must reviews and analyzes information system audit records for indications of inappropriate or unusual activity.			Report findings of inappropriate or unusual activity to incident response team.
Monthly					
Vulnerability Scanning	RA-5d	CSPs should mitigate all discovered high-risk vulnerabilities within 30 days. CSPs should send their ISSO updated artifacts every 30 days to show evidence that outstanding high-risk vulnerabilities have been mitigated.			
Continuous Monitoring Security State	CA-7d	CSPs must report the security state of the system to their own organizational officials on a monthly basis.			
Access Records	PE-8b	CSPs must review visitor access records monthly.			
Vulnerability Scanning	RA-5a	CSPs must scan operating systems/infrastructure monthly. All scan reports must be sent to the ISSO.	✓		

Control Name	Control ID	Description	CSP Authored Deliverable	3PAO Authored Deliverable	Notes
Flaw Remediation	SI-2(2)	CSPs should use an automated mechanism to look for system flaws at least once a month.			Examples of programs that look for system flaws could include program that: i) inspect log files looking for variances in normal behavior; ii) look for missing patches; iii) look for errors that indicate software bugs; iv) look for processing errors; v) look for indications for intrusions; vi) look for malware; vii) look for access control violations or attempted violations etc..
Software & Information Integrity	SI-7(1)	CSPs must perform integrity scans monthly.			
Quarterly					
Wireless Access Restrictions	AC-18(2)	CSPs must monitor for unauthorized wireless connections.			Scan wireless access points and determine if any are unauthorized.
Publicly Accessible Content	AC-22d	CSPs must review content on publicly accessible system and look for non-public information.			This means you are looking for data leaks and erroneous or unauthorized information disclosure.
Plan of Action & Milestones	CA-5	CSPs must update the POA&M as needed, and must submit it to the ISSO quarterly.	✓		Self-Attestation § 3.3 Updates should be based on the findings from security assessments, security impact analyses, CSP risk assessments, continuous monitoring activities and any other indications of a security weakness.
Access Restrictions for Change	CM-5(5)b	CSPs must review and reevaluate their information system developer/integrator privileges quarterly. Record the date of the review in the *System Security Plan*.			

Control Name	Control ID	Description	CSP Authored Deliverable	3PAO Authored Deliverable	Notes
Least Functionality	CM-7(1)	CSPs must review the information system quarterly to identify and eliminate unnecessary functions, ports, protocols, and/or services. If ports, protocols, and/or services are changed, Table 10-4 in the *System Security Plan* should be updated at the time of change. Changes should be made according to the CSP change management process that is described in the *Configuration Management Plan*.			
Vulnerability Scanning	RA-5a	CSPs must scan web applications and databases quarterly. All scan reports should be sent to the ISSO.	✓		
Vulnerability Scanning	RA-5d	CSPs must mitigate all moderate-risk vulnerabilities within 90 days and must send their ISSO artifacts every 90 days to show evidence that outstanding moderate-risk vulnerabilities have been mitigated.			
Semi-Annually					
Monitoring Physical Access	PE-6b	CSPs must review physical access logs semi-annually. Record the dates of review in the *System Security Plan*.			Self-Attestation § 3.10
Annually					
Information Security Policies	All "-1" Controls	CSPs must review Information Security Policies and Procedures annually. Insert the updated Policy document as an Attachment to the *System Security Plan* and submit the updated plan to the ISSO one year from the Provisional Authorization date and each year thereafter.	✓		Self-Attestation §3.12 All control families have "-1" controls (e.g. AC-1, SC-1).

Control Name	Control ID	Description	CSP Authored Deliverable	3PAO Authored Deliverable	Notes
Account Management	AC-2j	CSPs must perform an annual review and re-certification of user accounts to verify if the account holder requires continued access to the system. Record the date of annual user re-certification in the *System Security Plan*.			It is advisable to develop and document the annual user re-certification process and plan.
Security Awareness	AT-2	CSPs must provide basic security awareness training to all users annually. Record the date that security awareness training last took place in the *System Security Plan*.			Self-Attestation § 3.7 Security awareness training should include contractors, executives, and anyone who has access to the system.
Auditable Events	AU-2(3)	CSPs must review and update auditable events annually. Changes to the auditable event list should be recorded in the *System Security Plan*. CSPs should record the date that the auditable event review meeting takes place in the *System Security Plan*. Meeting notes with information about who attended the meeting should be archived.			This activity should also be performed whenever there is a change in the threat environment whether self-detected, or communicated by the JAB (via the ISSO).

Control Name	Control ID	Description	CSP Authored Deliverable	3PAO Authored Deliverable	Notes
Security Assessments	CA-2b	CSPs must have a 3PAO assess a subset of their security controls annually. Submit the assessment report to the ISSO one year from the Provisional Authorization date and each year thereafter.		✓	Self-Attestation §3.11 Consult with the ISSO to obtain information on which controls to assess during annual testing. Deliverables produced by 3PAOs are always separate from deliverables produced by CSPs.
Continuous Monitoring	CA-7(2)	CSPs must track, assess, and monitor their compliance with all vulnerability mitigation procedures annually. Record the date of the review in the *System Security Plan*.			
Continuous Monitoring	CA-7(2)	CSPs must require unannounced penetration testing to occur annually to ensure compliance with all vulnerability mitigation procedures. All penetration testing reports must be sent to the ISSO.		✓	Self-Attestation §3.8 Deliverables produced by 3PAOs are always separate from deliverables produced by CSPs.
Baseline Configuration and System Component Inventory	CM-2(1)a	CSPs must review and update the baseline configuration annually or during installations and updates. Changes and updates to the baseline configuration should be made in accordance with the change control process described in the CSP's *Configuration Management Plan*.			This activity should also be performed whenever there is a significant change to the system.

Control Name	Control ID	Description	CSP Authored Deliverable	3PAO Authored Deliverable	Notes
Configuration Management Plan	CM-9	CSPs must review and update the *Configuration Management Plan* annually. Submit the new plan to the ISSO at the time of annual Self-Attestation one year from the Provisional Authorization date (and each year thereafter).	✓		Self-Attestation § 3.9
IT Contingency Plan	CP-2d	CSPs must review and update the *IT Contingency Plan* annually. Submit the new plan to the ISSO at the time of annual Self-Attestation one year from the Provisional Authorization date (and each year thereafter).	✓		Self-Attestation § 3.6
IT Contingency Training	CP-3	CSPs must train personnel in their contingency roles and responsibilities annually. Record the date of the training in the *System Security Plan*.			
IT Contingency Plan Testing & Exercises (Moderate Systems)	CP-4a	CSPs must test and exercise the *IT Contingency Plan* (for Moderate systems) every year. Insert a new *IT Contingency Plan Test Report* into Appendix F of the *IT Contingency Plan* (which is submitted annually).	✓		Self-Attestation § 3.6 Moderate systems require functional testing and exercises.
Information System Backup	CP-9(1)	CSPs must test backups annually to verify integrity and reliability. When the *System Security Plan* is updated annually, this control description should indicate when (date) the last test took place and who performed the testing.			

Control Name	Control ID	Description	CSP Authored Deliverable	3PAO Authored Deliverable	Notes
Incident Response Training	IR-2b	CSPs must conduct incident response training annually. When the *System Security Plan* is updated annually, this control description should indicate when training took place, training materials, who participated, and who conducted the training.			
Incident Response Testing	IR-3	CSPs must perform incident response testing annually. When the *System Security Plan* is updated annually, record the results of the incident response testing directly in the control description box indicating when testing took place, testing materials, who participated, and who conducted the testing.	✓		Self-Attestation § 3.2 Test all contact information in the Appendices of the *Incident Response Plan* to make it is accurate.
Incident Response Plan	IR-8c	CSPs must review the *Incident Response Plan* annually and update it if necessary. Insert the updated Incident Response Plan as an attachment to the *System Security Plan*.	✓		Self-Attestation § 3.2
Physical Access Authorizations	PE-2c	CSPs must review physical access authorization credentials annually and remove personnel from the access list who no longer require access. The date at which this review takes place, and who performed it, should be recorded in the *System Security Plan*.			Self-Attestation § 3.10
Physical Access Control	PE-3f	CSPs must inventory physical access devices annually. The date of the inventory should be recorded in the *System Security Plan*.			Self-Attestation § 3.10

Control Name	Control ID	Description	CSP Authored Deliverable	3PAO Authored Deliverable	Notes
Physical Access Control	PE-3g	CSPs must change combinations and keys annually. The date that the keys and combinations are changed should be recorded in the *System Security Plan* along with the name of the person responsible for making the changes.			Self-Attestation § 3.10 This activity should also be performed when keys are lost, combinations are compromised, or individuals are transferred or terminated.
System Security Plan	PL-2b, c	CSPs must review and update the *System Security Plan* annually. Submit the new plan to the ISSO at the time of the annual Self-Attestation one year from the Provisional Authorization date (and each year thereafter).	✓		Self-Attestation § 3.5 Table 9-1 in the *System Security Plan* must be updated.
Access Agreements	PS-6b	CSPs must review and update access agreements annually. The date of the access agreement review should be recorded in the *System Security Plan*.			A good time to do this is during the annual user re-certification (AC-2j).
Vulnerability Scan	RA-5a	CSPs must have an accredited 3PAO scan operating systems/infrastructure, web applications, and databases annually. All scan reports must be sent to the ISSO.		✓	Deliverables produced by 3PAOs are always separate from deliverables produced by CSPs.
Boundary Protection	SC-7(4)e	CSPs must remove traffic flow that is no longer supported by a business/mission need. Changes and updates to traffic flow should be made in accordance with the change control process described in the CSP's *Configuration Management Plan*.			Table 1-4 in the *System Security Plan* should be updated to reflect any changes.
Every Three Years					
Security Training	AT-3b	CSPs must provide role-based security training every three years. The date that the training took place, along with who provided the training, should be recorded In the *System Security Plan*.			Role-based security training is typically for privileged users.

Control Name	Control ID	Description	CSP Authored Deliverable	3PAO Authored Deliverable	Notes
Security Training Records	AT-4b	CSPs must archive security training records for three years. In the *System Security Plan*, record who participated in training and when the training took place. Archive the actual training materials.			
Security Authorization	CA-6c	The security authorization will be re-evaluated by the JAB at least every three years. CSPs should record the date of the Provisional Authorization, and any reauthorization, in the *System Security Plan*.			This activity should also be performed whenever there is a significant change to the system.
IT Contingency Plan Testing & Exercises (Low Systems)	CP-4a	CSPs should test and exercise the *IT Contingency Plan* (for Low systems) every three years. Record the testing date in the *System Security Plan* and submit the test results with the annual Self-Attestation.	✓		Self-Attestation § 3.6
Position Categorization	PS-2c	CSPs should review position categorizations every three years. Record the date that position categorization was completed in the *System Security Plan*.			
Risk Assessment	RA-3c, d	CSPs should review and update security assessments every three years and record the date of the last security assessment in the *System Security Plan*.			This activity should also be performed whenever there is a significant change to the system.
Every Five Years					
Personnel Screening	PS-3b	Law enforcement must undergo personnel screening every 5 years. Any law enforcement staff screened should have the screening date recorded in the *System Security Plan* along with their name.			High impact personnel screening is not required at this time because FedRAMP is not supporting high impact sensitive systems at this time.

6. ANNUAL SELF-ATTESTATION

Delivery of continuous monitoring artifacts must be provided by the CSP as part of the annual self-attestation process. FedRAMP has developed a Self-Attestation Template and CSPs must fill out this template and provide named artifacts prior to reauthorization.

An effective continuous monitoring program requires periodic review of security policies, planning activities, and security procedures and processes. The review and update of these areas are built into various document templates such as the System Security Plan, and therefore, they are not called out as separate self-attestation deliverables.

The following sections describe the deliverables named in the FedRAMP Self-Attestation Template and provide instructions and background information on each deliverable.

6.1 Self-Attestation: Incident Reporting

As incidents occur and are reported, CSPs should maintain records on who the incident was reported to and when the incident was reported. Further, as part of their Incident Handling activities, CSPs should conduct an in-house incident investigation, perform analysis on the incident, determine the cause, eradicate any intruders or malware, and implement preventive measures. The Self-Attestation Template requires CSPs to include a summary of reported incidents. CSPs should fill out the summary table based on their own incident records.

6.2 Self-Attestation: Incident Response Test Report

It is important for CSPs to periodically test their Incident Response Plan to identify the effectiveness of the plan and any potential weaknesses or deficiencies that need to be corrected. FedRAMP security control IR-3 requires that CSPs test their Incident Response Plan annually. For systems that have achieved a FedRAMP Provisional Authorization, test plans should be submitted prior to testing to the FedRAMP ISSO for review and approval by the JAB.

The CSP should describe what aspects of the test they intend to measure, whether the plan will represent a tabletop exercise, a simulation, or a comprehensive exercise. The CSP should use the results of this test to perform modifications to existing security procedures, technology implementations, and training of staff. It is expected that deficiencies noted from the tests may appear as planned actions for resolution on the CSP's Plan of Action & Milestones. Each test should look for weaknesses identified in prior testing to ensure that those weaknesses were properly corrected.

Once incident response testing has been completed, the CSP should develop a report that includes the outcome and results of the testing. Deficiencies in the incident response process, controls, implementation or documentation should be cited in the report. The date of the test, the

participants, and the test location should all be noted in the report. Tasks related to these deficiencies that have been added to the POA&M should be noted. The report, identified as the annual *Incident Response Test Report* should be attached to the Self-Attestation.

6.3 Self-Attestation: POA&M Update

The *Plan of Action & Milestones* (POA&M) document serves as a high-level work plan to correct weaknesses in the CSP's security implementation. The POA&M identifies and lists weaknesses discovered through security assessments, annual continuous monitoring activities, or any other method. FedRAMP provides a POA&M template for CSPs which is available on www.FedRAMP.gov.

FedRAMP security control CA-5 requires CSPs to update their POA&Ms on a quarterly basis. Updated POA&Ms need to be submitted quarterly to the system ISSO. During the annual Self-Attestation, only the most recent POA&M should be submitted. The ISSO reviews POA&Ms for unacceptable risk exposure. Unresolved POA&M items and elevated risk posture presented by new vulnerabilities are escalated to the JAB by the ISSO by as necessary.

6.4 Self-Attestation: Vulnerability Scan Reports

CSPs are required to scan infrastructure and operating systems monthly, and web applications and databases quarterly, in accordance with the FedRAMP Security Control Baseline (RA-5a). Scans should also be performed after a significant environmental or system change to identify any vulnerability exposed as a result of the change. These scans are intended to inform the CSP of known vulnerabilities in their service offering that are susceptible to exploits to the detriment of agency data. Findings that are identified from the vulnerability scanning should be categorized and included on the POA&M. Remediation plans should be subsequently implemented.

Scans can also be run to identify policy compliance. Different systems may require different scanning tools to identify vulnerabilities. Scanning tools should be selected for the particular component within the CSP's environment that will be scanned. Not all scanners have the ability to perform vulnerability detection for all components. Scanners are typically designed to test particular system components such as networking equipment, operating systems, application servers, web servers, web applications, and database servers. Select the right scanner for the job. FedRAMP does not offer recommendations on which scanners to use.

All scan reports must be submitted to the designated FedRAMP ISSO. Both 3PAOs and ISSOs will review the scan reports against the declared asset inventory to ensure compliance with the RA-5a control. CSPs will be required to update the POA&M and submit the new POA&M to the ISSO (a quarterly requirement). ISSOs will review the results of the scans against the POA&M, and will make recommendations to the JAB regarding the ongoing Provisional Authorization.

6.5 Self-Attestation: Unnannounced Penetration Testing

At a minimum of once annually, CSPs must require that their 3PAO performs unannounced penetration testing. 3PAOs should use the SAP and SAR templates for the annual unnannounced penetration testing.

6.6 Self-Attestation: Update System Security Plan

CSPs must review and update their System Security Plan (SSP) annually. Additionally, in the event of significant change within the security authorization boundary or in a control implementation, the SSP should be reviewed and updated. The plan must be kept current and accurately describe implemented system controls and reflects change to the system and its environment of operation. This review and update of the SSP is designed to allow for a CSP to holistically review the control implementations and update the policy and procedures to ensure an effective security program. The updates should consider as many data points as possible in the review, but at a minimum should include the following:

- Updated POA&M items and remediation steps
- Changes in implementation as a result of Incident Response Testing
- Updates to hardware and software used in the system
- Results of annual penetration testing
- Results of vulnerability scanning
- And other risk assessment activities.

During this update, certain controls must be reviewed and updated as identified in the FedRAMP security control baseline. These updates are designed to make sure that the information represented by the CSP is current and up to date. Table 4 in section 5.4 includes a list of those controls. In addition to updating the controls within the SSP, evidentiary artifacts should be provided showing compliance with the control. The updated SSP will be submitted to the FedRAMP office annually.

6.7 Self-Attestation: IT Contingency Planning & Testing

On an annual basis, the Contingency Plan must be reviewed and updated to reflect current operating conditions within the CSP's infrastructure. The Contingency Plan must be tested in accordance with the appropriate impact level identified in the FedRAMP Security Baseline. At the low impact level, contingency plans must be tested once every three years and may be tested through tabletop exercises. At the moderate impact level, contingency plans must be tested annually through a functional exercise.

CSPs must develop their test plans and have those test plans approved by FedRAMP prior to execution. Test plans should be developed in accordance with NIST SP 800-84 (as amended). FedRAMP will review these test plans in accordance to determine if the availability of the system and organization during a contingent event can be gauged as a result of the exercise.

Upon approval of the test plan, the CSP can then conduct the exercise. The exercise results should be provided in a test report. Weaknesses or deficiencies identified through the test should

be added to the POA&M and appropriate steps and countermeasures implemented to mitigate or remediate each weakness or deficiency. The testing and reports should be prepared in accordance with NIST SP 800-84.

6.8 Self-Attestation: IT Security Awareness Training Record

CSPs are expected to provide ongoing IT security and awareness training to personnel servicing the system. This training should be designed to provide general awareness of common threats to IT security, to address CSP specific concerns and policies to create a vigilant workforce. Best practices include periodic testing and retraining on areas of focus of the CSP's workforce.

To measure the consistency of this training program, a CSP is required to provide training records on an annual basis. These training records identify the personnel that have been trained, the dates they were trained and the subject areas that training covered. This information is used by FedRAMP to understand the awareness of the personnel of the CSP.

7. ASSISTANCE WITH INCIDENT RESPONSE

The shared tenant architecture of cloud services implies that a single incident may impact multiple federal agencies leveraging the cloud services. It is a FedRAMP requirement that CSPs obtain assistance with incidents from their customer agencies and from US-CERT. Obtaining assistance starts with reporting incidents. Working as a team, agencies, CSPs, and US-CERT are positioned to handle and resolve incidents faster than if each entity worked on incidents alone.

7.1 Preparing for Incidents

It is a requirement for all CSPs to develop an *Incident Reponses Plan*. The *Incident Response Plan* is required by security control IR-8 and the plan needs to be reviewed and updated annually. CSPs should include in the *Incident Response Plan* a list of three key contacts that customer agencies can call upon for the purpose of incident response coordination. One of the contacts should include a 24 x 7 operations center at the CSP that is always reachable. Aside from the three key contacts, contact information for all incident response team members should be included in an Appendix of the *Incident Response Plan*.

CSPs should attach their updated *Incident Response Plan* to their *System Security Plan* prior to sending the *System Security Plan* to the ISSO during the annual self-attestation.

7.2 How CSPs Report Incidents

When a CSP detects an incident, it should be reported to affected customer agencies based on the categorization of the incident. The incident categories and reporting times are described in NIST SP 800-61, Revision 1, Appendix J. Only incidents that fall into categories 1 through 4 should be reported.

Note: NIST SP 800-61, Revision 1, *Computer Security Incident Handling Guide*

can be found at the following URL:
http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf.

All incidents need to be documented and tracked as required by security control IR-5. If CSPs have reported the incident to affected customer agencies, and have not yet been contacted by US-CERT and require immediate assistance, the CSP should contact US-CERT directly using the online reporting form at https://forms.us-cert.gov/report/. At the same time that the CSP reports incidents to agency customers, the CSP should also report the incident to their FedRAMP assigned ISSO.

7.3 How Agencies Report Incidents

When a CSP reports an incident to an affected agency, the agency will escalate incidents to US-CERT according to the agency's own respective *Incident Response Plan* instructions. If an agency discovers an incident that has not been reported to them by the CSP, the agency should contact the CSP using the incident contact information provided in the CSP's *Incident Response Plan*.

Agencies should offer to coordinate assistance between US-CERT and CSPs when CSPs report incidents to agencies. If a CSP reports an incident to an agency, and the agency escalates the incident to US-CERT, the agency should forward to US-CERT the *Incident Reporting Form* that was filled out by the CSP.

7.4 Incident Handling

Security control IR-4 requires CSPs to employ incident handling techniques and processes. CSP incident handling capabilities required by this control should be documented in the *Incident Response Plan*. Though CSPs should be fully capable to handle incidents, in coordination with their customer agencies, CSPs may also obtain additional assistance from US-CERT.