Guide for Determining Eligibility and Requirements for the Use of Sampling for Vulnerability Scans

Version 1.0

March 20, 2018

FedRAMP

DOCUMENT REVISION HISTORY

DATE	VERSION	PAGE(S)	DESCRIPTION	AUTHOR
03/20/2018	1.0	All	Initial document	FedRAMP PMO

ABOUT THIS DOCUMENT

This document provides guidance on determining eligibility and complying with the Federal Risk and Authorization Management Program (FedRAMP) requirements for use of sampling in vulnerability scanning.   This document applies to Cloud Service Providers (CSPs) to determine whether sampling is appropriate for their environment.

This document is not a FedRAMP template – there is nothing to fill out in this document.

This document uses the term *authorizing official (AO)*. For systems with a Joint Authorization Board (JAB) provisional authorization to operate (P-ATO), AO refers primarily to the JAB unless this document explicitly says *Agency AO*. For systems with a FedRAMP Agency authorization to operate (ATO), AO refers to each leveraging Agency's AO.

WHO SHOULD USE THIS DOCUMENT?

This document is intended to be used by CSPs (interested in determining whether sampling is appropriate for their environment and CSPs approved to use vulnerability sampling), a CSP's designated FedRAMP Point of Contact (POC), 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 a continuous monitoring program.

HOW TO CONTACT US

Questions about FedRAMP or this document should be directed to info@fedramp.gov.

For more information about FedRAMP, visit the website at http://www.fedramp.gov.

TABLE OF CONTENTS

1. PURPOSE

The purpose of this document is to describe the FedRAMP requirements for the optional use of sampling in vulnerability scanning for Cloud Service Providers who choose to use sampling to meet FedRAMP continuous monitoring requirements as opposed to 100% scanning as defined in the *FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide*. The document is also used as a first step by the CSP to determine whether sampling is appropriate for their environment. Vulnerability scanning in this context includes all scanning required by the FedRAMP PMO for the FedRAMP Continuous Monitoring Program.

2. FEDRAMP REQUIREMENTS FOR VULNERABILITY SCANS

In order to respond to customers' rapidly changing demands for increases and decreases in cloud resources in this environment, the CSP must maintain rigid change management processes and highly automated mechanisms for deploying system images in large geographically dispersed production environments. This leads to establishing a very short list of standard system images that make up the *unique inventory*. Usually, vulnerability scans are performed on 100% of these assets, but because of the high fidelity of system configurations across the environments, the scan results of a subset of components can be used to ascertain the state of the entire population. Therefore, a sampling of the assets within each of the standard system images is considered sufficient; a 3PAO must attest that the sample selected is sufficient to represent the state of the unique inventory. Additionally, the AO must approve the sample methodology.

A *unique inventory item* is a grouping of one or more discrete inventory assets that are managed as a single asset class. For example, 1,000 servers deployed using the same system build or system image release are considered to be a single, unique inventory item, even if that system build has been updated and only a subset of the 1,000 servers is running the newest version, because the servers are being managed as a single asset class. In these cases, the configuration management plan must identify how the CSP is managing the inventory items and asset classes, ensuring all assets are updated within an appropriate/approved amount of time (limiting the number of different builds/versions in a given asset type). Unique inventory items must be defined as part of the Vulnerability Sampling Plan reviewed by the 3PAO.

This guidance applies to system builds that are deployed from standard images (that must remain unchanged when pushed to and running on subsequent devices or machines in production) to general purpose servers in highly dynamic virtual, and some physical, environments. The guidance also applies to operating systems deployed to network devices, web applications, databases, and other software products where appropriate.

CSPs that are currently conducting approved vulnerability sampling that does not conform with this vulnerability scan requirements guide have six months from the publication of this guide to update their vulnerability scanning processes and Vulnerability Sampling Plan to align with this document. These plans must be submitted to the FedRAMP PMO for review and approval. CSPs will continue meeting their ongoing FedRAMP continuous monitoring requirements using approved vulnerability scanning methodologies during this review and approval period.

FedRAMP vulnerability scanning guidelines require at least monthly scans of 100% of inventory components. Vulnerability scanning using sampling targets the same component asset categories but instead requires scanning of a sample attested to represent the unique inventory by a 3PAO and approved by the AO. Given the risk, FedRAMP recommends that externally accessible (outside of the boundary, without the use of a VPN) system components do not use this sampling methodology; 100% of externally accessible system components should be scanned, using a scanning technology appropriate for the access type (web scanners for web endpoints and portals, network scanners for operating systems, etc.).

3. VULNERABILITY SCAN REQUIREMENTS FOR SAMPLING

The following steps are required for the CSP and 3PAO to ensure that an appropriate Vulnerability Sampling Plan is implemented, a *unique inventory* is maintained, components are appropriately selected, scans are performed, and results are reviewed and remediated:

1. **Comply with FedRAMP Requirements for Vulnerability Scans**
   - *FedRAMP JAB Vulnerability Scan Requirements Guide*
2. **Activate Capabilities to Ensure Unique Inventory Items are Identical**
   - The CSP will activate a method to demonstrate that all individual assets in a class are identical; within operational and management parameters.
   - The CSP will provide, to the 3PAO, a description of the product/method for ensuring unique inventory items are configured appropriately. The CSP will perform a test of the solution to demonstrate effectiveness annually, at time of FedRAMP Annual Assessment of the system, and provide the results to the 3PAO.
3. **Develop Vulnerability Sampling Plan**
   - Establish a Plan (methodology) by which sampling will be used; the Plan shall be reviewed at least annually, and maintained current.
   - Describe how components will be selected. Justify how the unique inventory item (such as a network device OS version) is built from a standard image and meets the intent of this guideline.
   - Ensure at each selection interval (each month when scans are run), that the assets are selected randomly from the total inventory. Describe the randomization method.
   - Describe how this sample effectively represents the entire inventory and satisfies the intent of vulnerability scan requirements.
4. **Establish *Unique Inventory* and Samples:**
   - Establish a list of the *unique inventory*.
   - Ensure each unique inventory item is based on system builds that are deployed from standard images (that must remain unchanged when pushed to and running on subsequent devices or machines in production) to general purpose servers in highly dynamic virtual, and some physical, environments. This also applies to operating systems deployed to network devices, web applications, databases, and other software products where appropriate.

- Select a sample sufficient to represent the unique inventory item. The sample must be attested to by a 3PAO at the time of the FedRAMP Annual Assessment.
  - Should the unique inventory change during the year, the CSP will update the Vulnerability Sampling Plan, including documenting how these devices continue to implement previously approved change, deviation, and security controls. 3PAOs will perform an assessment over the changed inventory at the time of the next FedRAMP Annual Assessment.
  - FedRAMP recommends that 100% of externally accessible (outside of the boundary, without the use of a VPN) system components be scanned. However, if a sampling methodology is approved, there should be a strong justification, given the potential risk.

5. **Analyze Scan Results:**
   - Analyze the scan results to determine whether there was any variance in findings among components within the same *unique inventory* group outside of documented operational or management parameters. All unexpected variances within a unique inventory group must be discussed with the AO with the next Plan of Action and Milestones (POA&M). If applicable, a high-risk POA&M item should be created to investigate and explain why the variance occurred, and correct the unexpected variance. At the discretion of the AO, if the sampling methodology is found to be inefficient (whether through one variance, or multiple variances), the AO may rescind sampling approval, requiring 100% scanning.

6. **Justify Appropriateness of CSP's Participation in "Sampling:"**
   - Prior to acceptance to participate in sampling, the CSP should provide a convincing justification that participation is appropriate. This justification should reference all implemented controls that demonstrate adherence with the principles and requirements contained within this vulnerability scan sampling guide, enabling successful adherence to FedRAMP vulnerability scanning requirements testing using sampling.

7. **Assessment and Attestation by 3PAO and Approval of Authorization Official:**
   - The 3PAO will review the CSP's Vulnerability Sampling Plan, implementation and test results and attest to the sampling's effectiveness.
   - The AO for any agency issuing an ATO must approve the plan and justification, prior to participating in sampling.
   - Approval for using sampling can be rescinded by the AO due to identification of weaknesses in the plan, implementation or effectiveness, for example, if an anomaly was identified and a major issue was discovered during the investigation (as part of the high POA&M item).

APPENDIX A: FEDRAMP ACRONYMS

The *FedRAMP Master Acronyms & Glossary* contains definitions for all FedRAMP publications, and is available on the FedRAMP website Documents page under Resources Documents.

(https://www.fedramp.gov/documents/)

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.