FedRAMP Deviation Request Form
INSTRUCTIONS

PLEASE REMOVE THE INSTRUCTIONS BEFORE SUBMITTING FORM.

WHO SHOULD USE THIS FORM?

Cloud Service Providers (CSPs) with systems that have an existing FedRAMP authorization, seeking approval from FedRAMP related to a false positive (FP), operationally required (OR) risk, or risk adjustment (RA) related to a vulnerability identified as part of assessment or continuous monitoring activities.

ABOUT THIS FORM

When the CSP identifies a vulnerability that potentially warrants different handling than normally required by FedRAMP, the CSP may submit a deviation request to FedRAMP using this form. Deviation request types include:

- **False Positive (FP)**: A finding that incorrectly indicates a vulnerability is present, where none actually exists. Justified through documentation and evidence.
- **Risk Adjustment (RA)**: A reduction in the scanner-cited risk level of a finding. Accomplished through existing or new compensating controls that reduce likelihood and/or impact of exploitation.
- **Operational Requirement (OR)**: A finding that cannot be remediated, often because the system will not function as intended, or because a vendor explicitly indicated it does not intend to offer a fix to their product. FedRAMP will not approve an OR for a High vulnerability; however, the vendor may mitigate the risk
- **RA & OR**: A single DR may simultaneously justify a risk adjustment and an operational requirement.

NOTE: A vendor Dependency does not require a deviation request.

For more information about deviation requests, see the *FedRAMP Continuous Monitoring Strategy Guide*.

FORM AND ATTACHMENT INSTRUCTIONS

FedRAMP adjudicates each DR individually. Please submit one form per DR.

1. Complete the form and attach additional pages if necessary.
2. Upload either a digitally signed copy, or a physically signed and scanned copy to OMB MAX.
3. Send a notification message to your FedRAMP POC or info@fedramp.gov - include the OMB MAX location.

NOTE: The CSP may mark the FP, OR, or RA as "Pending" after they submit the DR, while waiting for FedRAMP adjudication; however, they may only treat the vulnerability differently after FedRAMP approves the DR.

FedRAMP ACRONYMS

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

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

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

HOW TO CONTACT US

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

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

FedRAMP Deviation Request Form

Instructions:

1. Complete the form and attach additional pages if necessary.
2. Upload either a digitally signed copy, or a physically signed and scanned copy to OMB MAX.
3. Send a notification message to info@fedramp.gov - include OMB MAX location of the document.

CSP Contact Information

Company Name				
System Name				
Primary POC	Name		Title	
	Phone		Email	

Vulnerability Information *(Include only one POA&M item per DR submission.)*

POA&M ID		Scan ID	
Assets Impacted			
Vulnerability Name		**Vulnerability Source**	
Initial Rating *(please choose from drop down menu)*	Click to Choose	**Detection Date**	
Tool-provided Vulnerability Description			
Tool-provided Recommended Action			
CSP-provided Additional Vulnerability Information *(Optional)*			

Deviation Request Summary

DR Number		DR Submission Date	
Type of DR *(please choose from drop down menu)*	Click to Choose		
DR Rationale			

Additional Information: False Positive *(Complete this section only if you are submitting a false positive DR)*	
Evidence Description	
List of Evidence Attachments *Attach evidence, such as screen shots. List evidence attachments here.*	
Additional Information: Operational Requirement *(Complete this section if you are submitting an operational requirement or a risk reduced operational requirement DR.)*	
Operational Impact Statement *Explain the limitations that prevent the vulnerability from being fixed. Include negative operational impacts of remediation.*	
Justification *For a Moderate vulnerability that is not being mitigated to Low, explain why the authorizing official should accept the risk without mitigating it.*	
List of Operational Requirement Attachments *Attach evidence, such as screen shots. List evidence attachments here.*	

Additional Information: Risk Reduction

(Complete this section if you are submitting a risk reduction or a risk reduced operational requirement DR.)

Complete all fields below. Include references to the System Security Plan as applicable

To complete the fields in this section, use the CVSS Environmental Score Metrics definitions found here: https://nvd.nist.gov/vuln-metrics

Attack Vector Click to Choose Item *Describe whether local access, physical access, or network access is required for vulnerability exploitation. Describe how, based on the CSP's implemented security model, the necessary access is reduced or not available.*	Delete prior to submission: For example, a vulnerability may require adjacent network access (as determined by following the decision tree above) for exploitation and the vulnerability was discovered on a management network. The management network may be restricted to three administrators only, who only connect via a jumphost via specific dedicated workstations. The management network is only accessible via the jumphost and has no other connectivity to or from networks that are not managed directly. The previous example explains why the level of network access necessary for vulnerability exploitation is reduced or not available based on the CSP's implemented design since the vulnerable machines cannot be accessed via the network directly.
Attack Complexity Click to Choose Item *Low attack complexity means that an attacker can exploit the vulnerability at any time, at all times. High attack complexity means that a successful attack depends on conditions outside of the attacker's control.*	Delete prior to submission: For example, normally a vulnerability may be exploitable 100% of the time which would be Low attack complexity. However, in the CSP's environment, you have implemented security controls which add conditions outside of the attacker's control such as containerized or sandboxed applications or mandatory access controls.
Privileges Required Click to Choose Item *No privileges required can be exploited by an unauthorized user. Low privileges require a normal authenticated user to exploit the vulnerability. High privileges require an Administrator or System level authenticated user to exploit the vulnerability.* *Describe any security controls that prevent or reduce the likelihood of a vulnerability exploitation attempt having the required privileges on the system.*	Delete prior to submission: For example, if the vulnerability requires Low privileges, however only Administrators can access the vulnerable systems, then the likelihood of exploitation is reduced since there are no non-trusted users on the system(s). If the vulnerability does not require privileges and the CSP has limited access to the system to only specific hosts, which reduces the likelihood of exploitation.

User Interaction Click to Choose Item *Describe any security controls that prevent or reduce the likelihood of necessary user interaction on the system.*	Delete prior to submission: For example, if user interaction is required to exploit a vulnerability by clicking on a URL and the CSP has disabled the ability for users to click on URLs and have programs automatically load those URLs, then that control would prevent or reduce the likelihood of the necessary user interaction on the CSP's affected system(s).
Impact Metrics: Confidentiality Click to Choose Item *High if all information is disclosed to an attacker or some critical information is disclosed. Low if some information can be obtained and/or the attacker does not have control over the kind or degree. None if no information is disclosed.*	Delete prior to submission: For example, if the vulnerability were exploited on the vulnerable system, the impact to Confidentiality and Integrity would be None since all data at rest and in transit is encrypted with a FIPS 140-2 validated algorithm. In addition, the vulnerable systems do not contain data at rest. If the vulnerability were exploited on the vulnerable system, the impact to availability would be None as other VMs would automatically be spawned to accept the workload. This would be transparent to the user.
Impact Metrics: Integrity Click to Choose Item *High if an attacker can modify information at any time or only some critical information can be modified. Low if some information can be modified and the attacker does not have control over the kind or degree. None if there is no integrity loss.*	

Impact Metrics: Availability Click to Choose Item *High if an attacker can cause a resource to become completely unavailable or if the resource is a critical component and can become partially available. Low if an attacker can cause reduced performance or interrupt resources availability or response. None if there is no availability impact.*	
Remediation Level Click to Choose Item *"Official fix" means that a complete vendor solution is available; either the vendor has issued an official patch, or an upgrade is available. "Temporary fix" means that there is an official but temporary fix available. This includes instances where the vendor issues a temporary hotfix, tool, or workaround. "Workaround" means that there is an unofficial, non-vendor solution available. In some cases, users of the affected technology will create a patch of their own or provide steps to work around or otherwise mitigate the vulnerability. "Unavailable" means that there is either no solution available or it is impossible to apply.* *Describe any remediation that has been taken to address the vulnerability on the affected system(s).*	Delete prior to submission: For example, an "Official fix" has been provided by the vendor and the CSP has tested it in their development environment. During testing, the CSP noted that a critical service became unavailable once the patch was added. This was confirmed on a separate test system with the same result occurring. The CSP provides evidence of the result. The CSP has instead followed a "workaround" solution to mitigate the risk of vulnerability exploitation.

FedRAMP Deviation Request Form

List of Risk Reduction Attachments *Attach evidence, such as screen shots. List evidence attachments here.*	
Additional Information	
Please use the space to the right to provide any additional information you believe is relevant to this devitation request.	
CSP Signature *(To be signed by an individual with the authority to represent the CSP to FedRAMP)*	
Name *(Type)*:	Title:
____ Signature	__________________________________ Date