Information Security Risk Acceptance Recommendation Form

This Acceptance of Risk (AOR) expires 12 months from the approval date or sooner if the following take place: new vulnerabilities are identified, system changes or remediations have been implemented, or there is a change to existing security controls.

Submit by Email

Contact Information

Last Name

First Name

Science Event Number

Project Name

Email Address

Phone Number

System Information

Host Name

IP Address

Services Running on the System

Operating System

Function of the System to Support the Project

Risk Information

Describe the risk as defined by the vulnerability scan description.

Describe the impact of the risk based on the position of the system in the USAP environment.

Describe the risk to the impacted system, project, user community, and the USAP mission if the risk is accepted and the vulnerability is not remediated.

Describe the impact of not remediating the item as it relates to the function of the system.

Describe the impact to the system, project, user community, and the USAP mission if the risk is not accepted by the NSF, and immediate remediation efforts are deemed necessary for continued network connectivity.

Risk to the USAP network if the NSF accepts the risk.

Risk to the system and project if the NSF accepts the risk.

Level of Impact on the project if the risk is not accepted

Level of Effort to remediate the vulnerability.

Describe mitigating controls currently in place that lower the impact of the risk to the system and the USAP network. List mitigation and remediation strategies that can be implemented to lower the impact of the risk to the system and the USAP network. Include a timeline for implementing recommended mitigations and remediations.