Date:	07/02/2025
From:	Coalfire Systems, Inc.
To:	FedRAMP PMO
Subject:	Coalfire - Paramify FedRAMP 20x Validated Assessment

Coalfire Systems, Inc. (“Coalfire”), an American Association for Laboratory Accreditation (A2LA) accredited FedRAMP Third-Party Assessment Organization (3PAO), has partnered with Paramify to perform a FedRAMP 20x Validated Assessment. The objective of the assessment is to demonstrate compliance with Key Security Indicators (KSIs) established by FedRAMP for the 20x Phase One Pilot and to work towards FedRAMP authorization. Assessment activities took place between 06/25/2025 and 07/02/2025.

Assessment activities were primarily performed directly within the Paramify web application. Paramify has developed a specific FedRAMP 20x program within the application that uses Paramify Risk Solutions to demonstrate compliance with KSIs. Risk Solutions are various security capabilities that are then mapped to various requirements. In this case those requirements are the FedRAMP 20x KSIs. Paramify has developed more than 290 unique Risk Solutions, of these 56 are mapped into the KSIs to detail how Paramify is securing their cloud service offering (CSO).

Coalfire’s methodology for the FedRAMP 20x Validated Assessment is based on completeness, accuracy, timeliness, and exceptions when it comes to the automated and manual demonstration of the KSIs. To establish completeness, Coalfire reviewed the inventory and the scripts used to generate it to ensure that the list of applicable resources has been identified. To establish accuracy, Coalfire reviewed the evidence provided within the application and ensured that the evidence derived from scripts, integrations, and documentation was representative of the asset inventory. To establish timeliness, the application maintains timestamps to ensure that evidence is relevant and that activity against requirements is tracked. To handle exceptions, Paramify allows for evidence, comments, and references to be added to each KSI implementation. Paramify reflects the status for each KSI that is displayed on the program dashboard.

Based on the results of the assessment activities Coalfire has produced human-readable and machine-readable assessment reports. These reports detail the status of each KSI validation (True, False, Partial) and provide details on the tests and evidence reviewed by Coalfire in determining implementation status. All evidence was reviewed directly within the Paramify Cloud. Provided below are the example Data Dictionary and Output:

Data Dictionary:

{
"Evidence ID": Internal Coalfire Evidence Indicator,
"Evidence Title": Title of the evidence request,
"Evidence Description": Longer description of the evidence requests to meet the requirements listed in the “Requirements” field,
"Evidence Domain": Coalfire defined domain for organization purposes and mapping to other frameworks,
"Evidence Category": Coalfire defined category for organization purposes and mapping to other frameworks,
"Requirements": FedRAMP requirements that the control pertains to and may be more exhaustive than minimum requirements for current baseline.
"Compliance Status": True=Compliance, False=Non-Compliant, Partial=Partially Compliant
"Test Method": Automated, AI-Validated, Manual
"Senior Assessor": Last Name, First Name of the Senior Assessor responsible for validation
"Date Tested": Date Coalfire tested the CSP controls
},

Example Output:

[

{
"Evidence ID": 22,
"Evidence Title": "Information security policies and procedures",
"Evidence Description": "Documented and approved information security policies and procedures which are the overarching or governing policies for the information security program. The policies and procedures including their associated periodic review and approval histories.",
"Evidence Domain": "Governance Risk Compliance",
"Evidence Category": "Governance Risk Compliance Policy and Procedure",
"Requirements": "AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1, AC-18, CM-4, MA-2, MA-5, PE-13, PS-7, RA-7, SA-4, SA-4(10), SA-9, SC-13, SC-28, SC-28(1), SC-8, SC-8(1), SR-1, SR-2",
"Compliance Status": "Partial",
"Test Method": "AI-Validated",
"Senior Assessor": "Last, First",
"Date Tested": "1/1/25"
},
{
"Evidence ID": 711,
"Evidence Title": "Privileged account request for transferred employee",
"Evidence Description": "Supporting records demonstrating privileged account requests for transferred employees.",
"Evidence Domain": "Identity and Access Management",
"Evidence Category": "New User Account and Credential Provisioning",
"Requirements": "AC-2, IA-4, IA-5, IA-5(1)",
"Compliance Status": "False",
"Test Method": "Automated",
"Senior Assessor": "Last, First",
"Date Tested": "1/1/25"
},
{
"Evidence ID": 1,
"Evidence Title": "Production environment MFA requirements",
"Evidence Description": "Output from cloud service provider configurations to demonstrate that MFA is enabled to access the production environment.",
"Evidence Domain": "Identity and Access Management",
"Evidence Category": "Multifactor Authenticators",
"Requirements": "AC-17, SC-12",
"Compliance Status": "True",
"Test Method": "Automated",
"Senior Assessor": "Last, First",
"Date Tested": "1/1/25"
}

]

Sincerely,

Jorden Foster
Senior Director
FedRAMP Assessment Services
Coalfire Systems, Inc.