FedRAMP

Developer Data Bites

May 11, 2023

GSA

info@fedramp.gov

fedramp.gov

Introduction

Purpose: To create space for dialogue between developers who use OSCAL and the FedRAMP® automation team.

Outcomes:

- Shared understanding of the repository and validation changes coming with the Rev 5 transition.
- Productive discussion around OSCAL

Agenda:

- Welcome
- Pre-Submitted Q&A
- Repository and Validation Changes with Rev 5 Transition
- Open Forum
- Next Steps & Closing

Data Bites Guiding Principles

Keep the discussion respectful

Be curious, seek understanding

Speak from your own experience

Challenge through questions

Focus on ideas

Keep it technical

Pre-Submitted Questions

Pre-Submitted Questions

Question (Issue #398):

Requesting the inclusion of a new prop in the FedRAMP baseline profile that includes the previous assessment procedures from the FedRAMP Security Test Case Procedures template to support users who are transitioning from the manual submission process to the OSCAL method.

e.g.

```
 <part id="ac-1.a.1_obj.2" name="objective">

  <prop ns="https://fedramp.gov/ns/oscal"
        name="response-point"
        value="You must fill in this response point."/>
  <prop name="method" class="fedramp" value="EXAMINE"/>
  <prop name="label" value="AC-1(a)(1)[2]"/>
  <prop name="assessment-procedure" ns="toolvend0r.xxx" value="AC-1.a.1.2"
  <p>defines personnel or roles to whom the access control policy are to be disseminated;</p>
</part>
```

FedRAMP does not preclude OSCAL solution providers from including properties of their own as long as they are tagged with an alternate namespace. The current Schematron validations will not flag props that are part of alternative namespaces. This will allow vendors to implement whatever mechanisms they deem appropriate for transition between manual and automated submissions.

Pre-Submitted Questions

Question (Issue #405):

For JAB authorization, when applying for the initial JAB P-ATO, the RAR must first be completed, and is valid for 1 year.
The OSCAL models provided by FedRAMP do not include reference to which controls are required for RAR, and which are for SAP and SAR. Is there going to be a model for the RAR, so CSPs can submit the RAR through OSCAL and attain the P-ATO?

It is currently not supported at the moment, but could be an interesting use case and perhaps something for the future if GSA would like to pursue. Escalating to PMO review team SMEs for consideration. Note: Potential future enhancement.

FedRAMP Automation GitHub Updates

Update on FedRAMP automation repository

10x Flexion Transition

- 10x/Flexion team has transitioned the majority of Schematron validations support but is still available for consultation to FedRAMP team for limited period of time.
- Surge of tickets recently related to POAM and SAR issues.

Issues/Ticket Tags

- **Newly opened issues this cycle**
  - #406 - validate_with_schematron.sh script failures.
  - #407 - Validating SAP, SAR and POAM using Fedramp Validation code
  - #409- 415 - (Investigations in progress)
- **Closed issues this cycle related to Schematron Validations**
  - #405 - RAR submission for OSCAL (Readiness Assessment Report)

Repository and Validation Changes with Rev 5 Transition

Repository and Validation Changes with Rev 5 Transition

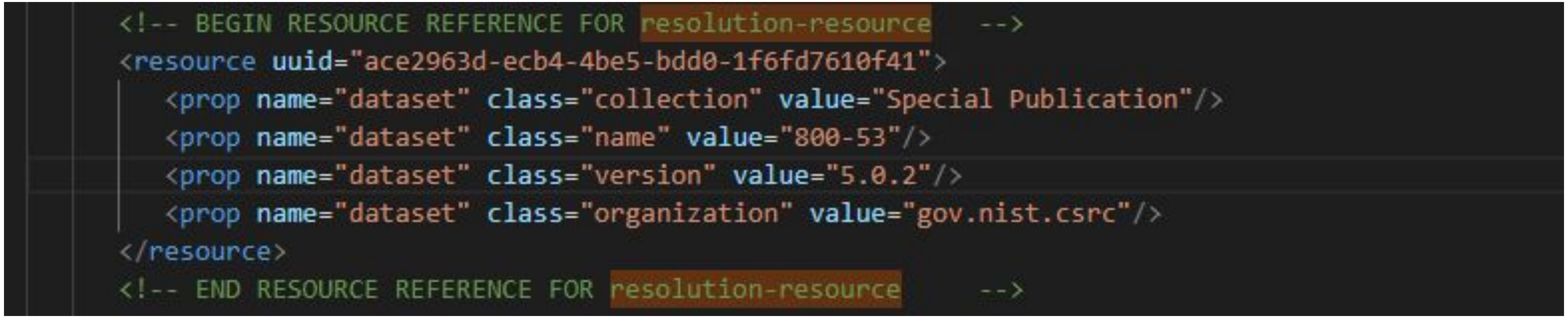
Overview of Changes

- Legacy submissions (FYI):
  - Format of word template are changing for Rev 5.
  - Certain artifacts will be included within the Rev 5 SSP template that were not included in Rev 4 template.
- Addition of new properties (props) to FedRAMP namespace.
- Breaking out of guidance and documentation into separate folders on Github
- Breaking out of templates, resources and baselines into separate folders on Github
- Separation of Schematron Rulesets
  - Ability to have separate rulesets between Rev 4 and Rev 5 (future revisions).
- Separation of Schematron Validation output verbiage and references.
  - SSP template and guidance changes require separate output language
- Removing Schematron Validation rules requiring submission of PIA/PTA and FedRAMP Laws and Regulations in OSCAL.

Repository and Validation Changes with Rev 5 Transition

New resolution-resource property

- Addition of a new property (prop) and back-matter resource reference in the FedRAMP namespace that will enable easy determination of the associated NIST 800-53 controls catalog that FedRAMP resolved-profile-catalogs were derived from.
- Enables automated support to determine which FedRAMP validation rulesets are to be used by validation code.

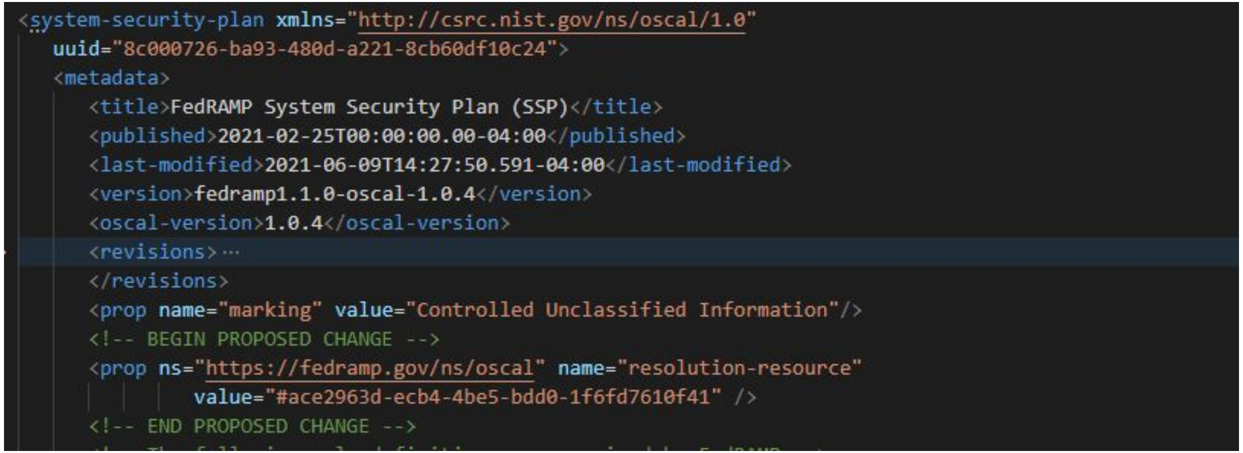


```
<!-- BEGIN RESOURCE REFERENCE FOR resolution-resource    -->
<resource uuid="ace2963d-ecb4-4be5-bdd0-1f6fd7610f41">
  <prop name="dataset" class="collection" value="Special Publication"/>
  <prop name="dataset" class="name" value="800-53"/>
  <prop name="dataset" class="version" value="5.0.2"/>
  <prop name="dataset" class="organization" value="gov.nist.csrc"/>
</resource>
<!-- END RESOURCE REFERENCE FOR resolution-resource      -->
```

Repository and Validation Changes with Rev 5 Transition

New resolution-resource property(cont.)

- New prop (resolution-resource) not required for rev 4 FedRAMP OSCAL submissions during transition period.
- New prop (resolution-resource) required for rev 5 FedRAMP OSCAL submissions.



```
<system-security-plan xmlns="http://csrc.nist.gov/ns/oscal/1.0"
  uuid="8c000726-ba93-480d-a221-8cb60df10c24">
  <metadata>
    <title>FedRAMP System Security Plan (SSP)</title>
    <published>2021-02-25T00:00:00.00-04:00</published>
    <last-modified>2021-06-09T14:27:50.591-04:00</last-modified>
    <version>fedramp1.1.0-oscal-1.0.4</version>
    <oscal-version>1.0.4</oscal-version>
    <revisions>···
    </revisions>
    <prop name="marking" value="Controlled Unclassified Information"/>
    <!-- BEGIN PROPOSED CHANGE -->
    <prop ns="https://fedramp.gov/ns/oscal" name="resolution-resource"
          value="#ace2963d-ecb4-4be5-bdd0-1f6fd7610f41" />
    <!-- END PROPOSED CHANGE -->
```

Repository and Validation Changes with Rev 5 Transition

GitHub Rev 4 vs. Rev 5

- Breaking out of guidance and documentation into separate folders on Github
  - Current: /fedramp-automation/documents
  - Future:
    /fedramp-automation/documents/rev4
    /fedramp-automation/documents/rev5
- Breaking out of templates, resources and baselines into separate folders on Github
  - Current: /fedramp-automation/dist/content/rev4
  - Future:
    /fedramp-automation/dist/content/rev4
    /fedramp-automation/dist/content/rev5
- Potential other breakouts pending...

Open Forum

Thank you

Our next Developer Data Bites virtual meeting will be on **Thursday, June 8, 2023 at 12p ET.**

Submit questions and future discussion topics to OSCAL@fedramp.gov

Learn more at fedramp.gov

@FEDRAMP

How to Submit Issues with FedRAMP

Ensuring your outstanding issues or questions are received:

Issues can be submitted in several ways:

✓ Preferred

Open an issue on fedramp-automation github so that it will benefit the NIST/FedRAMP community. https://github.com/GSA/fedramp-automation/issues

Alternate

Email us at oscal@fedramp.gov

OSCAL Resources

NIST:

https://pages.nist.gov/OSCAL/
Learning Resources: https://pages.nist.gov/OSCAL/learn/
Current release: https://github.com/usnistgov/OSCAL/releases
Development version: https://github.com/usnistgov/OSCAL/tree/develop
Content repo: https://github.com/usnistgov/oscal-content

FedRAMP:

Current repo: https://github.com/GSA/fedramp-automation
Current issues: https://github.com/GSA/fedramp-automation/issues
Validations work: https://github.com/18F/fedramp-automation/tree/master/src/validations
Web based validation tool:
https://federalist-2372d2fd-fc94-42fe-bcc7-a8af4f664a51.app.cloud.gov/site/18f/fedramp-automation/#/documents/system-security-plan

What topics do you want to see in the future?

Quick Poll

What do you want to see?

1.

Demonstration Information

Useful Links

3rd Party Tools

- https://www.oxygenxml.com/xml_editor/download_oxygenxml_editor.html (Oxygen XML Editor)
- https://github.com/usnistgov/OSCAL/tree/main/xml/schema (NIST xsd schemas)
- https://github.com/usnistgov/oscal-content/tree/main/nist.gov/SP800-53/rev4/xml (NIST profiles)
- https://github.com/GSA/fedramp-automation/tree/master/dist/content/rev4/baselines/xml (FedRAMP profiles)
- https://code.visualstudio.com/download (Visual Studio Code)
- https://marketplace.visualstudio.com/items?itemName=qub.qub-xml-vscode
- https://marketplace.visualstudio.com/items?itemName=redhat.vscode-xml

Rev 5 Update

Rev 5 Timeline

Estimated Release Date of XXXXXXX

- Phase 1 Release: XXXXXXX
  - Rev 5 Baselines
  - CSP Transition Plan
- Phase 2 Release: XXXXXXX
  - Templates
  - OSCAL Docs
- Phrase 3 Release: XXXXXXX
  - Everything else (+45 documents)