Virtual Room #3

Hosted By: **Jet Ryan**, Solutions Architect, *Telos Corporation*

(OSCAL Webpage)

Disclaimer: Portions of the event may be recorded and audience Q&A or comments may be captured. The recorded event may be edited and rebroadcasted or otherwise made publicly available by NIST. By attending this event, you acknowledge and consent to having your conversation recorded.

oscal2022@nist.gov
conferences@nist.gov

Getting a Head Start on Automating your FedRAMP ATO using OSCAL in Xacta360

March 2, 2022

Telos®

INTRODUCTION

Jet Ryan

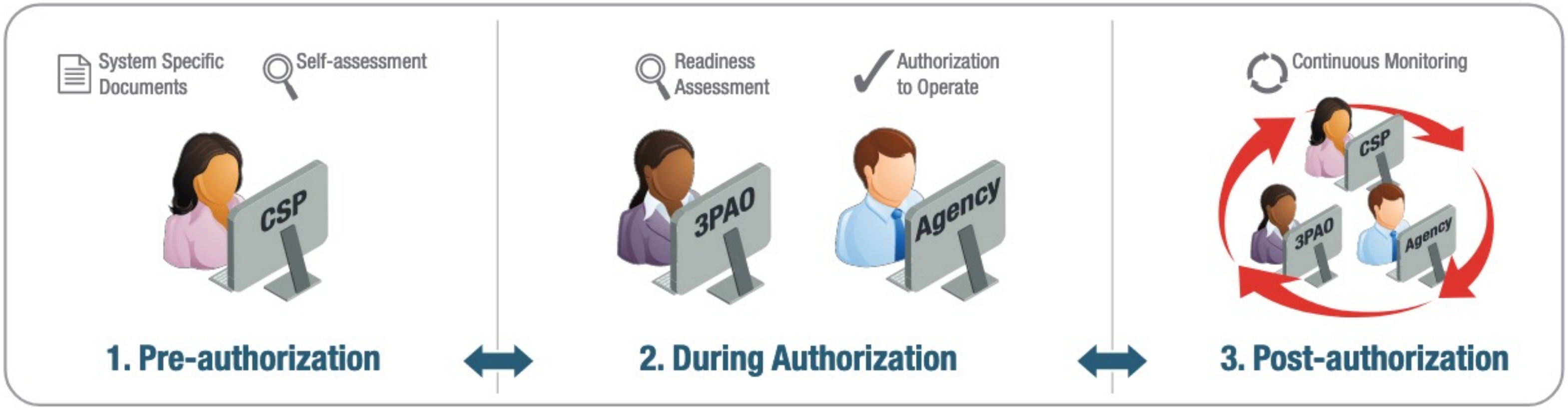
Solutions Architect - OSCAL Lead

Telos Corporation

Xacta® 360

XACTA® 360

- Xacta has existed as a compliance management platform since 2000
- Pre-built workflows for frameworks like FedRAMP and NIST RMF
- Customization without code, optimized for cloud security assessments
- Reduces time and dependencies in the assessment and authorization process



Telos

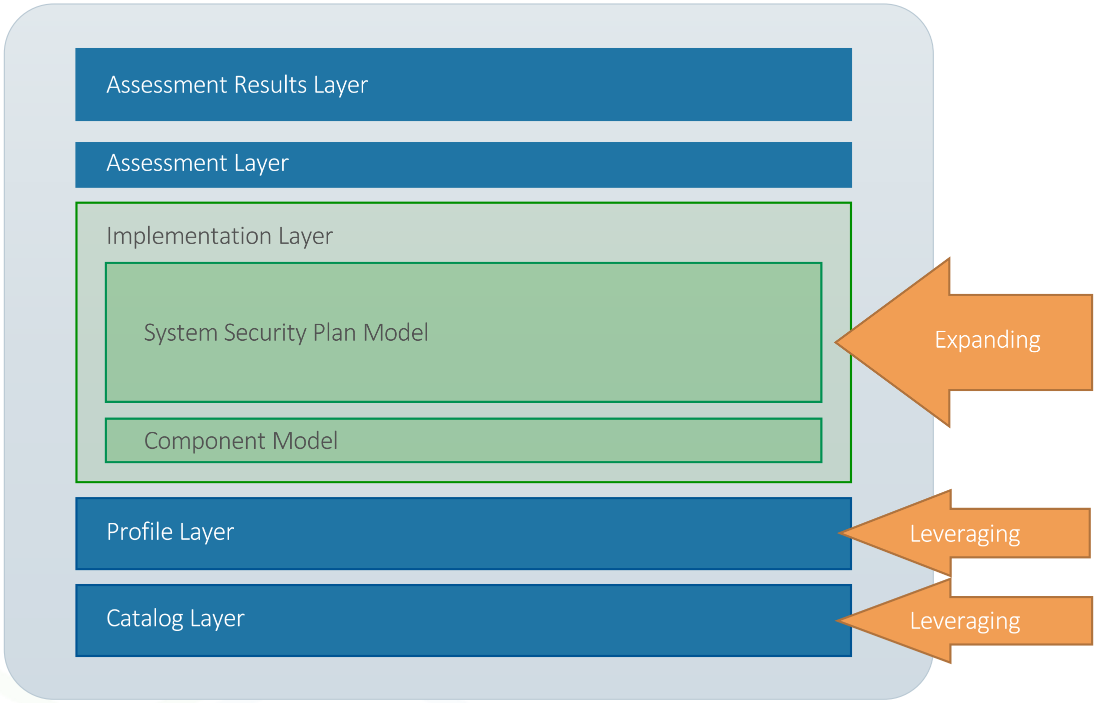
What’s Next?

How can we push the limits of compliance automation?

Our Vision: Accelerated ATO Enabled by OSCAL

- Open Security Control Assessment Language (OSCAL) is a data centric framework with the goal of standardizing the process for documenting and accessing security controls
- OSCAL enables movement at machine speed, allowing for faster authorization
- Advantages to roles across the authorization process
- Xacta360 will “hold the door open” to get users started in compliance as code
- Creation of “OSCAL enabled” workflows with pre-built mappings
- One click OSCAL export to generate an OSCAL package

Telos Support of OSCAL Layers and Initial Integration



OSCAL From the Bottom Up

- Xacta360 leverages OSCAL FedRAMP Controls Catalogs
- Xacta360 references OSCAL FedRAMP Baseline Profiles
- Started from SSP layer
- Plans are in motion to complete the SSP layer and interlink with other models

Current Release

- Mapped the OSCAL model for FedRAMP on the Xacta360 FedRAMP project
- Included the Metadata, System Characteristics, and System Implementation
  - Roles
  - System users
  - Ports, protocols, and services
  - Equipment inventory
  - System environment
  - Location
  - + more

In Development

- Inclusion of Controls implementation section
    - Responsible roles
    - Control parameters
    - Implementation status
    - Controls Origination
    - + more
- Resolve variation in control models
- Finalize what is accepted in terms of an OSCAL package

OSCAL Pipeline

Near future:

- Support controls catalog layer and profile layer on SSP export for dynamic OSCAL
- Completion of the SSP Layer with inclusion of Back-matter, import of profile, and leveraged authorizations

Beyond:

- Support control inheritance within OSCAL FedRAMP, BOE and XDE
- Support of other templates within OSCAL beyond FedRAMP
- Support the export of control, test, POA&M and risk artifacts within OSCAL
- Support of OSCAL import: profile and SSP layer

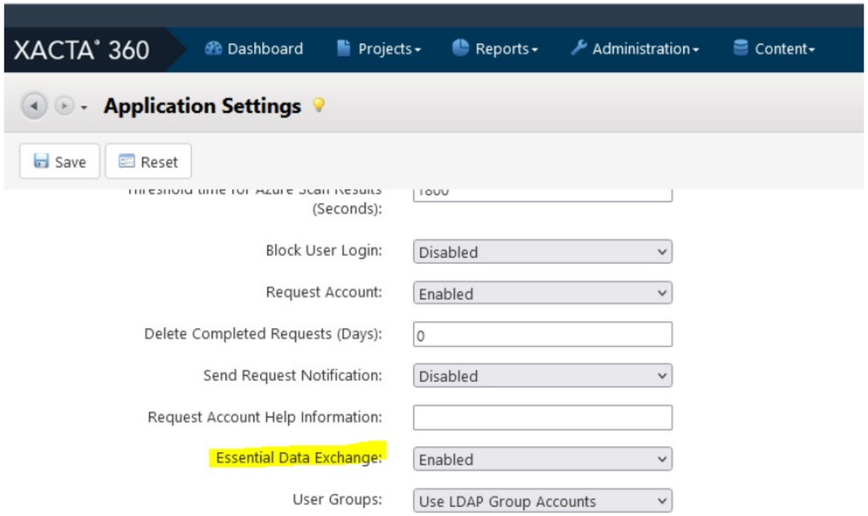
Head Start on the OSCAL package for FedRAMP

- What is generated from Xacta360 after an export?
  - Zip file containing FedRAMP SSP in OSCAL format
- What is required in an OSCAL Package for submission to FedRAMP?
  - FedRAMP SSP in OSCAL Format
  - Resolved OSCAL Profile
  - Controls catalog
  - Artifacts in back-matter

Xacta OSCAL Demo

Enable Data Exchange

Enabling Essential Data Exchange in Application Setting



Threshold time for Azure Scan Results (Seconds): 1800

Block User Login: Disabled

Request Account: Enabled

Delete Completed Requests (Days): 0

Send Request Notification: Disabled

Request Account Help Information:

Essential Data Exchange: Enabled

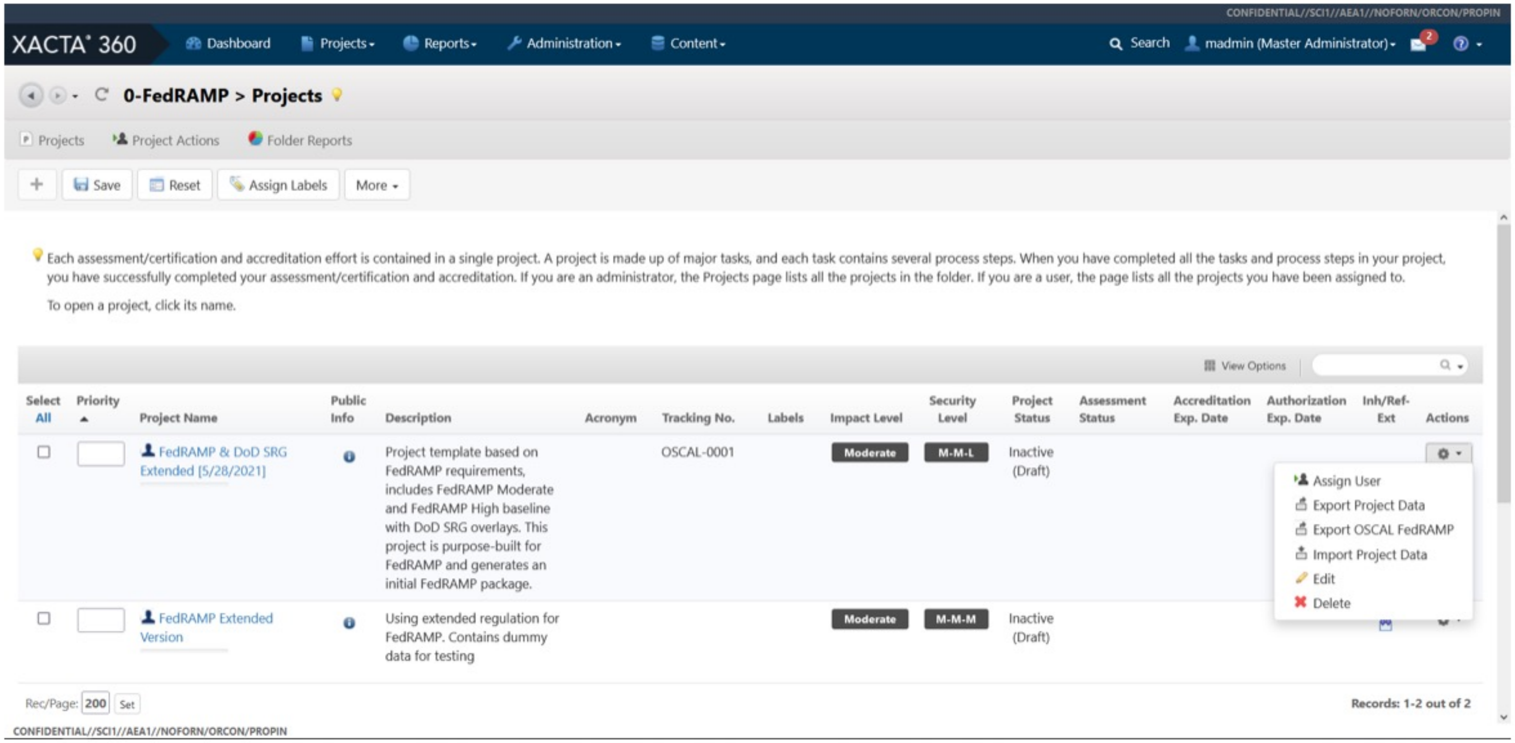
User Groups: Use LDAP Group Accounts

Application Setting Description of EDE

- **Essential Data Exchange** Essential Data Exchange allows master administrators to export projects to Body of Evidence (BOE) XML, (OSCAL) FedRAMP SSP XML, and Xacta Data Exchange (XDE) XML format. Mapping profiles for these formats can be created using the Administration > Application Settings > Essential Data Exchange Mappings page.

Navigate to Project, Select OSCAL Export

Project List Page Action Gear Icon



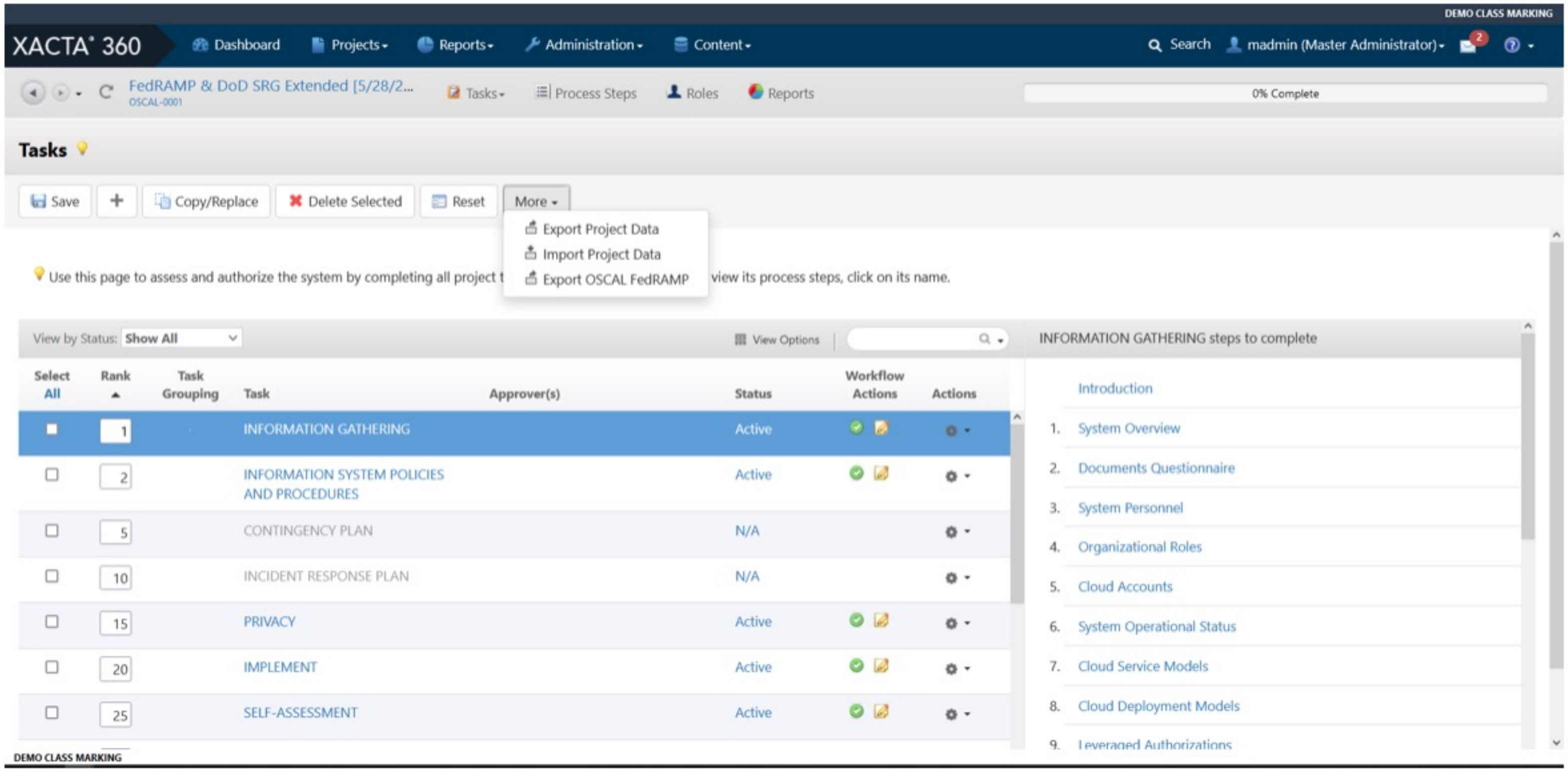
Each assessment/certification and accreditation effort is contained in a single project. A project is made up of major tasks, and each task contains several process steps. When you have completed all the tasks and process steps in your project, you have successfully completed your assessment/certification and accreditation. If you are an administrator, the Projects page lists all the projects in the folder. If you are a user, the page lists all the projects you have been assigned to.

To open a project, click its name.

Select All	Priority ▲	Project Name	Public Info	Description	Acronym	Tracking No.	Labels	Impact Level	Security Level	Project Status	Assessment Status	Accreditation Exp. Date	Authorization Exp. Date	Inh/Ref-Ext	Actions
□		FedRAMP & DoD SRG Extended [5/28/2021]	●	Project template based on FedRAMP requirements, includes FedRAMP Moderate and FedRAMP High baseline with DoD SRG overlays. This project is purpose-built for FedRAMP and generates an initial FedRAMP package.		OSCAL-0001		Moderate	M-M-L	Inactive (Draft)					
□		FedRAMP Extended Version	●	Using extended regulation for FedRAMP. Contains dummy data for testing				Moderate	M-M-M	Inactive (Draft)					

Can also Select from in Project

Task List Page "More" Dropdown



Tasks

Use this page to assess and authorize the system by completing all project t … view its process steps, click on its name.

Select All	Rank	Task Grouping	Task	Approver(s)	Status	Workflow Actions	Actions
☐	1		INFORMATION GATHERING		Active	✓	⚙
☐	2		INFORMATION SYSTEM POLICIES AND PROCEDURES		Active	✓	⚙
☐	5		CONTINGENCY PLAN		N/A		⚙
☐	10		INCIDENT RESPONSE PLAN		N/A		⚙
☐	15		PRIVACY		Active	✓	⚙
☐	20		IMPLEMENT		Active	✓	⚙
☐	25		SELF-ASSESSMENT		Active	✓	⚙

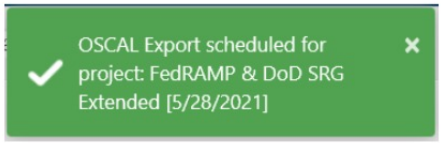
INFORMATION GATHERING steps to complete

Introduction

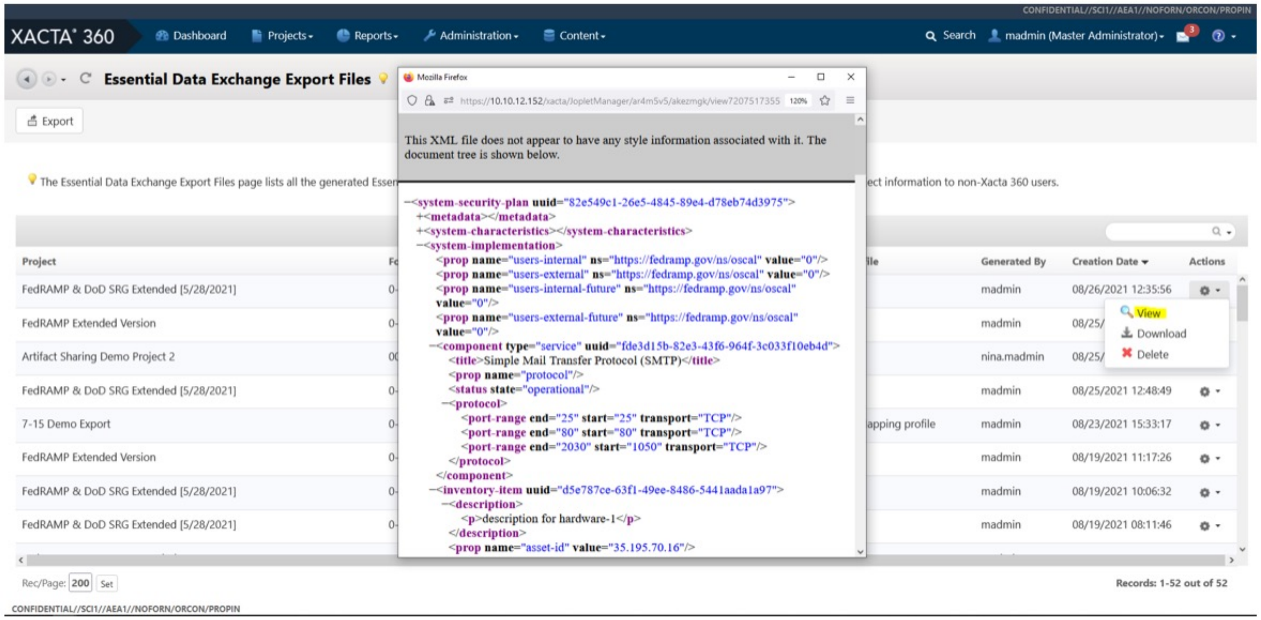
1. System Overview
2. Documents Questionnaire
3. System Personnel
4. Organizational Roles
5. Cloud Accounts
6. System Operational Status
7. Cloud Service Models
8. Cloud Deployment Models
9. Leveraged Authorizations

OSCAL Located Under Project Tab After Export Message Pops Up

Toaster Message when “Export OSCAL FedRAMP” is selected



OSCAL Export scheduled for project: FedRAMP & DoD SRG Extended [5/28/2021]



CONFIDENTIAL//SCI1//AEA1//NOFORN/ORCON/PROPIN

Essential Data Exchange Export Files

The Essential Data Exchange Export Files page lists all the generated Essen… …ect information to non-Xacta 360 users.

Project	F	…ile	Generated By	Creation Date	Actions
FedRAMP & DoD SRG Extended [5/28/2021]	0-		madmin	08/26/2021 12:35:56	⚙
FedRAMP Extended Version	0-		madmin	08/25/	
Artifact Sharing Demo Project 2	00		nina.madmin	08/25/	
FedRAMP & DoD SRG Extended [5/28/2021]	0-		madmin	08/25/2021 12:48:49	⚙
7-15 Demo Export	0-	apping profile	madmin	08/23/2021 15:33:17	⚙
FedRAMP Extended Version	0-		madmin	08/19/2021 11:17:26	⚙
FedRAMP & DoD SRG Extended [5/28/2021]	0-		madmin	08/19/2021 10:06:32	⚙
FedRAMP & DoD SRG Extended [5/28/2021]	0-		madmin	08/19/2021 08:11:46	⚙

Rec/Page: 200 Set

Records: 1-52 out of 52

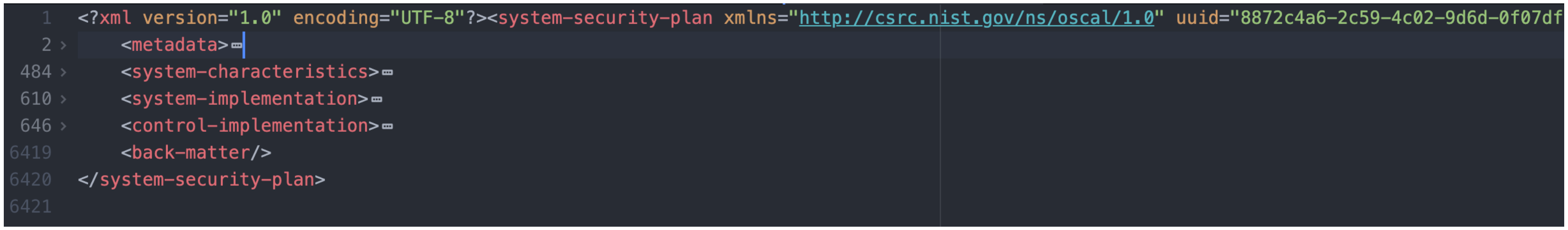
CONFIDENTIAL//SCI1//AEA1//NOFORN/ORCON/PROPIN

Mozilla Firefox
https://10.10.12.152/xacta/JopletManager/ar4m5v5/akezmgk/view7207517355
120%

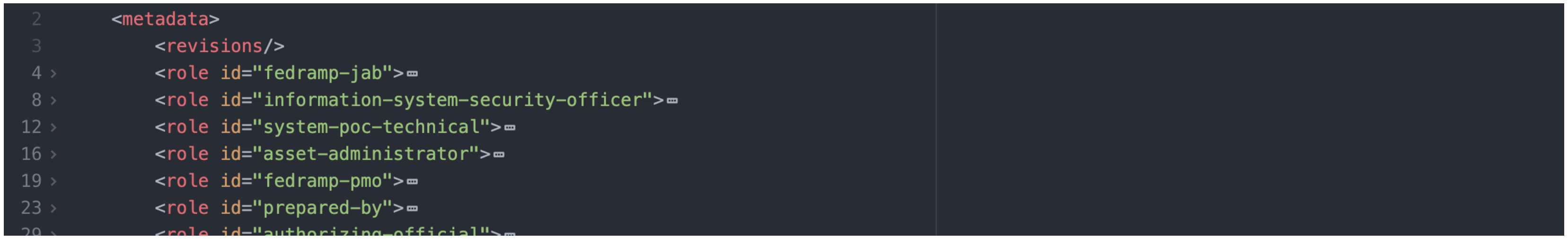
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
−<system-security-plan uuid="82e549c1-26e5-4845-89e4-d78eb74d3975">
  +<metadata></metadata>
  +<system-characteristics></system-characteristics>
  −<system-implementation>
     <prop name="users-internal" ns="https://fedramp.gov/ns/oscal" value="0"/>
     <prop name="users-external" ns="https://fedramp.gov/ns/oscal" value="0"/>
     <prop name="users-internal-future" ns="https://fedramp.gov/ns/oscal"
     value="0"/>
     <prop name="users-external-future" ns="https://fedramp.gov/ns/oscal"
     value="0"/>
    −<component type="service" uuid="fde3d15b-82e3-43f6-964f-3c033f10eb4d">
       <title>Simple Mail Transfer Protocol (SMTP)</title>
       <prop name="protocol"/>
       <status state="operational"/>
      −<protocol>
         <port-range end="25" start="25" transport="TCP"/>
         <port-range end="80" start="80" transport="TCP"/>
         <port-range end="2030" start="1050" transport="TCP"/>
       </protocol>
     </component>
    −<inventory-item uuid="d5e787ce-63f1-49ee-8486-5441aada1a97">
      −<description>
         <p>description for hardware-1</p>
       </description>
       <prop name="asset-id" value="35.195.70.16"/>
```

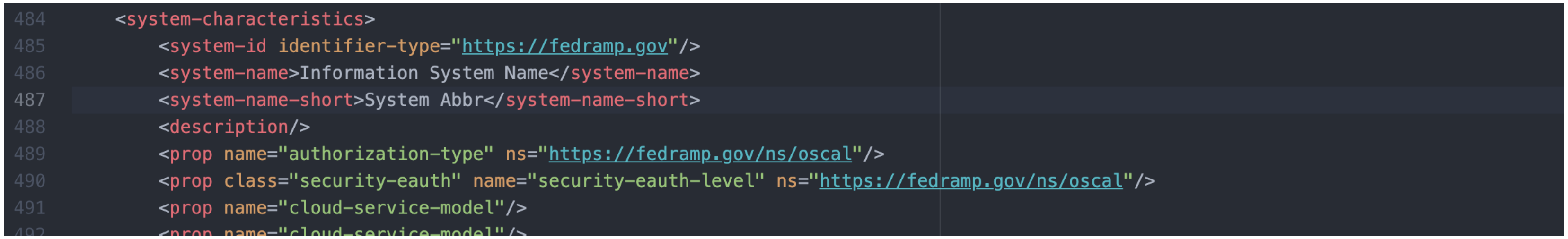
Open in OSCAL Tool or Text Editor



```
<?xml version="1.0" encoding="UTF-8"?><system-security-plan xmlns="http://csrc.nist.gov/ns/oscal/1.0" uuid="8872c4a6-2c59-4c02-9d6d-0f07df
    <metadata>⋯
    <system-characteristics>⋯
    <system-implementation>⋯
    <control-implementation>⋯
    <back-matter/>
</system-security-plan>
```

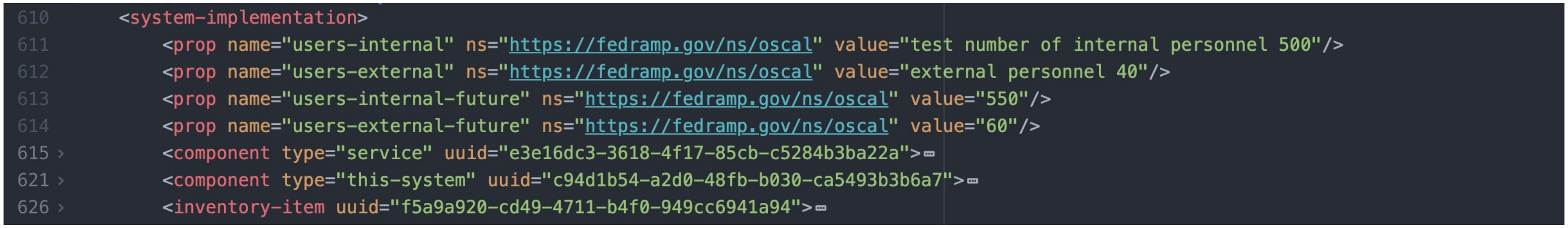


```
    <metadata>
        <revisions/>
        <role id="fedramp-jab">⋯
        <role id="information-system-security-officer">⋯
        <role id="system-poc-technical">⋯
        <role id="asset-administrator">⋯
        <role id="fedramp-pmo">⋯
        <role id="prepared-by">⋯
        <role id="authorizing-official">⋯
```

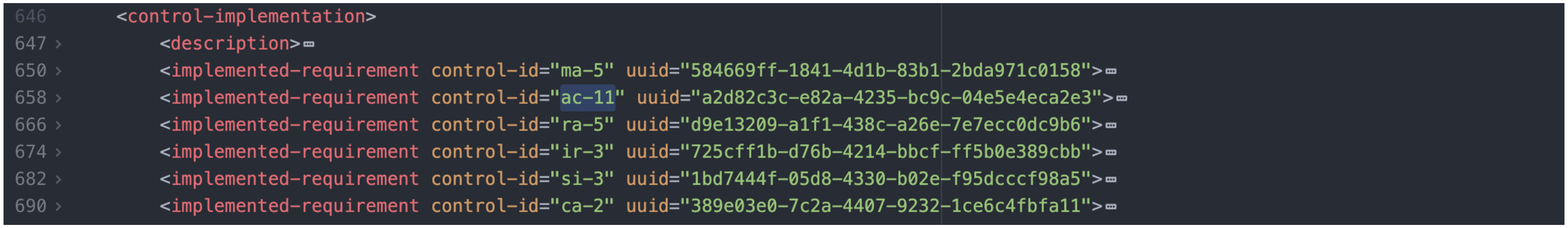


```
    <system-characteristics>
        <system-id identifier-type="https://fedramp.gov"/>
        <system-name>Information System Name</system-name>
        <system-name-short>System Abbr</system-name-short>
        <description/>
        <prop name="authorization-type" ns="https://fedramp.gov/ns/oscal"/>
        <prop class="security-eauth" name="security-eauth-level" ns="https://fedramp.gov/ns/oscal"/>
        <prop name="cloud-service-model"/>
        <prop name="cloud-service-model"/>
```

Open in OSCAL Tool or Text Editor



```
    <system-implementation>
        <prop name="users-internal" ns="https://fedramp.gov/ns/oscal" value="test number of internal personnel 500"/>
        <prop name="users-external" ns="https://fedramp.gov/ns/oscal" value="external personnel 40"/>
        <prop name="users-internal-future" ns="https://fedramp.gov/ns/oscal" value="550"/>
        <prop name="users-external-future" ns="https://fedramp.gov/ns/oscal" value="60"/>
        <component type="service" uuid="e3e16dc3-3618-4f17-85cb-c5284b3ba22a">
        <component type="this-system" uuid="c94d1b54-a2d0-48fb-b030-ca5493b3b6a7">
        <inventory-item uuid="f5a9a920-cd49-4711-b4f0-949cc6941a94">
```



```
    <control-implementation>
        <description>
        <implemented-requirement control-id="ma-5" uuid="584669ff-1841-4d1b-83b1-2bda971c0158">
        <implemented-requirement control-id="ac-11" uuid="a2d82c3c-e82a-4235-bc9c-04e5e4eca2e3">
        <implemented-requirement control-id="ra-5" uuid="d9e13209-a1f1-438c-a26e-7e7ecc0dc9b6">
        <implemented-requirement control-id="ir-3" uuid="725cff1b-d76b-4214-bbcf-ff5b0e389cbb">
        <implemented-requirement control-id="si-3" uuid="1bd7444f-05d8-4330-b02e-f95dcccf98a5">
        <implemented-requirement control-id="ca-2" uuid="389e03e0-7c2a-4407-9232-1ce6c4fbfa11">
```

Questions?

For more information on the topics we’ve discussed today:

Visit telos.com/xacta

Contact: sales@telos.com

Telos®

Solutions that empower
and protect the enterprise.™