

6. Leveraged FedRAMP-Authorized Services

The leveraged FedRAMP-Authorized services table is used to list both underlying leveraged authorizations, such as a SaaS running on an IaaS, and use of external cloud services with FedRAMP authorizations, such as a FedRAMP-authorized third party identity management service.

6 Leveraged FedRAMP-Authorized Services

The <Insert CSO Name> leverages the FedRAMP Authorized services depicted in Table 6.1 below.

Table 6.1 Leveraged FedRAMP Authorized Services

#	CSP/CSO Name (Name on FedRAMP Marketplace)	CSO Service (Names of services and features - services from a single CSO can be all listed in one cell)	Authorization Type (JAB or Agency) and FedRAMP Package ID #	Nature of Agreement	Impact Level (High, Moderate, Low, LI-SaaS)	Data Types	Authorized Users/Authentication

For each row in Table 6.1 there must be:

- a parties entry
- a leveraged-authorizations entry
- a components entry

parties Entry

A parties entry to indicate the organization that owns the leveraged system or external service

```
system-security-plan:
  metadata:
    parties:
      - uuid: 22222222-2222-4000-8000-004000000001
        type: organization
        name: Leveraged System Provider's Name
```

leveraged-authorizations Entry

The `leveraged-authorizations` entry must include:

- a `uuid`
- a `title` with the name of the system or service exactly as it appears in the FedRAMP Marketplace
- a `props` entry with:
 - `name` set to `package-id`
 - `ns` set to `http://fedramp.gov/ns/oscal`
 - `value` set to the package ID exactly as it appears in the FedRAMP Marketplace
- a `props` entry with:
 - `name` set to `security-sensitivity-level`
 - `ns` set to `http://fedramp.gov/ns/oscal`
 - `value` set to `fips-199-low`, `fips-199-modarete` or `fips-199-high` consistent with the FedRAMP Marketplace Information
- a `party-uuid` with the UUID of the `parties` entry above
- a `date-authorized` with the date listed in the FedRAMP Marketplace, expressed in [OSCAL date format](#).

FedRAMP Extensions

FedRAMP Extensions are defined when there is no way to represent required information using core OSCAL. They are depicted as properties (`props` entries) with a namespace (`ns`) value set to `http://fedramp.gov/ns/oscal`. Without the namespace, these properties may be ignored or flagged as invalid.

```
system-security-plan:
  system-implementation:
    leveraged-authorization:
      - uuid: 11111111-2222-4000-8000-019000000001
        title: CS0 Name
        props:
          - name: package-id
            ns: http://fedramp.gov/ns/oscal
            value: F9999999999
          - name: security-sensitivity-level
            ns: http://fedramp.gov/ns/oscal
```

```
value: fips-199-high
party-uuid: 22222222-2222-4000-8000-004000000001
date-authorized: '2015-01-01'
```

Allowed Values The FedRAMP extension `security-sensitivity-level`:

- `fips-199-high`
- `fips-199-moderate`
- `fips-199-low`

components Entry

The `components` entry must include:

- a `uuid`
- a `type` set to `system`
- a `title` set to the name of the leveraged system
- a `description` of the system. This is a core OSCAL requirement. FedRAMP has no specific requirement for the content of this field.
- a `props` entry with:
 - `name` set to `leveraged-authorization-uuid`
 - `value` set to the UUID of the `leveraged-authorization` entry above
- a `props` entry with:
 - `name` set to `nature-of-agreement`
 - `ns` set to `http://fedramp.gov/ns/oscal`
 - `value` set to `sla`, `contract` [needs more definition]
- a `props` entry with:
 - `name` set to `authentication-method`
 - `ns` set to `http://fedramp.gov/ns/oscal`
 - `value` set to the package ID exactly as it appears in the FedRAMP Marketplace
- One `props` entry for each "Data Type":
 - `name` set to `information-type`
 - `ns` set to `http://fedramp.gov/ns/oscal`
 - `value` set to the NIST SP 800-60 Volume 2 information ID
 - `class` set to `incoming` or `outgoing`
 - If the same information type is exchanged in both directions, there must be one `props` entry for incoming and a separate props entry for outgoing.
- The `status` assembly with the `state` field set to `operational`
 - For FedRAMP the value must always be operational; however, this is a required OSCAL field and cannot be omitted.

- One or more `responsible-roles` entries:
 - Identify the Provider (Required):
 - `role-id` set to `provider` (ensure `metadata` has a `roles` entry with `id` set to `provider`)
 - a `party-uuids` entry with the UUID of the `parties` entry defined above.
 - *Authorized Users*: One entry per authorized user type:
 - `role-id`
 - Use OSCAL-defined canonical values where appropriate.
 - If no canonical value exists, create an appropriate value that conforms with the [OSCAL token data type](#).
 - The value must also exist in the `metadata/roles` entries.

OSCAL Representation

```
system-security-plan:
  system-implementation:
    component:
      - uuid: 11111111-2222-4000-8000-009000100001
        type: system
        title: Leveraged Authorized System
        description: Briefly describe the leveraged system.

    props:
      - name: leveraged-authorization-uuid
        value: 11111111-2222-4000-8000-019000000001
      - name: nature-of-agreement
        ns: http://fedramp.gov/ns/oscal
        value: sla
      - name: authentication-method
        ns: http://fedramp.gov/ns/oscal
        value: 'yes'

      - name: information-type
        ns: http://fedramp.gov/ns/oscal
        value: C.3.5.1
        class: incoming
      - name: information-type
        ns: http://fedramp.gov/ns/oscal
        value: C.3.5.8
        class: outgoing

  status:
```

state: operational

responsible-roles:

- role-id: provider

party-uuids:

- 11111111-2222-4000-8000-c0040000000a

- role-id: asset-administrator

party-uuids:

- 11111111-2222-4000-8000-c0040000000a

FedRAMP Marketplace Information Matching

Information about *Leveraged FedRAMP Authorized Services* must match the content in the FedRAMP Marketplace. GSA updates a [JSON file](#) nightly that is used to render the FedRAMP Marketplace data.

OSCAL Field	GSA Field
CSP Name	/data/Providers/[#]/Cloud_Service_Provider_Name
CSO Name	/data/Providers/[#]/Cloud_Service_Provider_Package
Package ID	/data/Providers/[#]/Package_ID
Authorization Date	/data/Providers/[#]/Original_Authorization_Date
Impact Level	/data/Providers/[#]/Impact_Level

IMPORTANT FOR LEVERAGED SYSTEMS:

While a leveraged system has no need to represent content here, its SSP SHOULD include special inheritance and responsibility information in the individual controls. See the [Response: Identifying Inheritable Controls and Customer Responsibilities](#) section for more information.