Department of Justice
Office of the Chief Information Officer

Cyber Security Assessment & Management (CSAM)

Adopting OSCAL to Deliver the Latest NIST SP 800-53 Control Catalog to the CSAM Community

Cybersecurity Services Staff

CSAM Functionality and Benefits

Functionality	Benefits
Full end-to-end Assessment & Authorization management	Enterprise security risk visibility & awareness Automates ongoing authorization & assessment processes, supporting evolving OMB A-130 and FISMA requirements Monitors system Authorization to Operate (ATO) expirations, enhancing resource and budget allocation priorities Minimizes duplicative work by leveraging inheritance and hybrid security controls, reducing control assessment burden
Comprehensive view of FISMA System inventory and security posture with quantitative risk scoring	
Serves as organized repository for all required documentation	
Robust audit capability supporting internal and external audits	
Automation of System Security Plan (SSP) development and maintenance	
Provides for enhanced inheritance, hybrid controls, privacy controls	
Plan of Action & Milestones (POA&M) management	
Customizable dashboards, reports, & notifications	
Security control assessments with "motive" capability (e.g. A-123, core controls, privacy)	
Automated NIST 800-53 control-set migration	
Integration of NIST content supporting ATO processes	

CSAM Line of Business (LOB) Services and Benefits

Line of Business service	Benefit
DOJ hosting available	Alleviates maintenance/operation costs for LOB partner
Shared service model	Non-profit, cost recovery pricing structure
Partner community of cybersecurity subject matter experts Wide-ranging and ongoing integration capabilities	Continuous enhancements aligned with government cybersecurity requirements
Comprehensive implementation support	Tailored implementation & onboarding support for effective system utilization
Dedicated client engagement managers	Actively engages partner agency to provide guidance, gather feedback and assist in the growth of the application and customer
Helpdesk support	In-house tier 1, 2, and 3 support
Training	Regular user training and open forums, web-based and/or and on-site

CSAM and NIST SP 800-53

- The NIST SP 800-53 Security and Privacy Control catalog is a fundamental building block of the CSAM application

- Various iterations of CSAM have used the NIST publications dating back to SP 800-26 and the original SP 800-53 in the early-to-mid 2000's as the basis of their Control content
  - Prior to Revision 4, data load was done via manual data entry, copy/paste from PDF files

- CSAM Approach to Control Implementation and Assessment
  - Enterprise defines the importance and priority of each control
  - Systems select and describe the implementation of each control in narrative format
  - The assessment of each control drives its implementation status and residual risk analysis

- To support this approach, a control set in CSAM requires:
  - Controls from SP 800-53; and
  - Assessment Procedures from SP 800-53A
    - Also called "Determine If Statements" in CSAM

History of CSAM and NIST SP 800-53, Revision 4

April 2013

- NIST publishes SP 800-53, Revision 4 (Controls)

December 2014

- NIST publishes SP 800-53A, Revision 4 (Assessment Procedures)
- NIST publishes a machine-readable XML version

January 2015

- NIST publishes update to SP 800-53, Revision 4 (Controls)
- NIST publishes a machine-readable XML version
- CSAM team builds import logic to create the control set content for CSAM based on the 800-53 and 800-53A machine-readable XML files

March 2015

- CSAM team releases the NIST SP 800-53, Revision 4 control set with CSAM v3.4

Planning For NIST SP 800-53, Revision 5 in CSAM

September 2020

- NIST publishes SP 800-53, Revision 5 (Controls)

Spring 2021

- CSAM customers begin asking about status of the SP 800-53, Revision 5 control set
- OMB Circular A-130 requires federal agency legacy systems to be in compliance with new NIST standards and guidelines within one year of publication
- **Challenge:** CSAM's approach to control set content has a dependency on both the Controls (SP 800-53) and the Assessment Procedures (SP 800-53A)
  - SP 800-53, Revision 5 is final
  - SP 800-53A, Revision 5 is not yet final at this time
  - How do we support customers that need to use the Controls from SP 800-53, Revision 5 before SP 800-53A, Revision 5 is published?

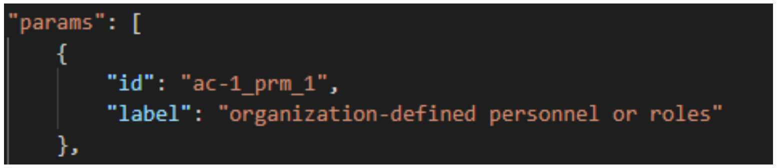
June 2021

- CSAM team releases the interim NIST SP 800-53, Revision 5 control set with CSAM v4.7, using Determine If Statements generated from the published OSCAL Rev5 Control Catalog

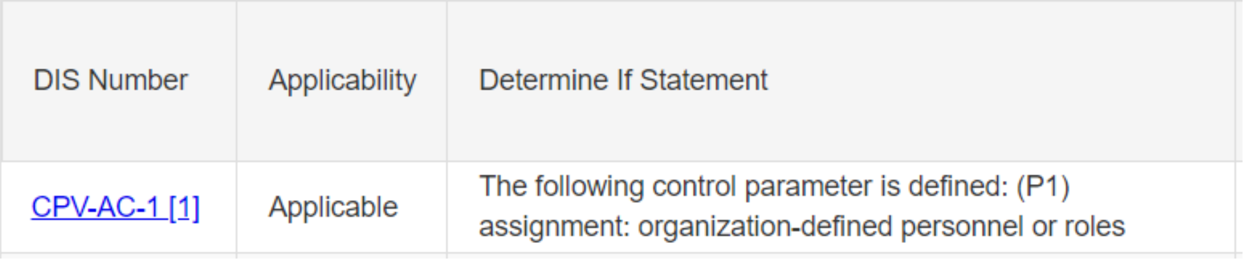
Interim Content Generated from OSCAL Catalog

The CSAM team processed the OSCAL Rev5 catalog (prior to the 800-53A assessment procedures being incorporated) to create the Determine If Statement content for CSAM that is comprised of two kinds of statements:

1. Statements covering the definition of each Control parameter (where applicable)



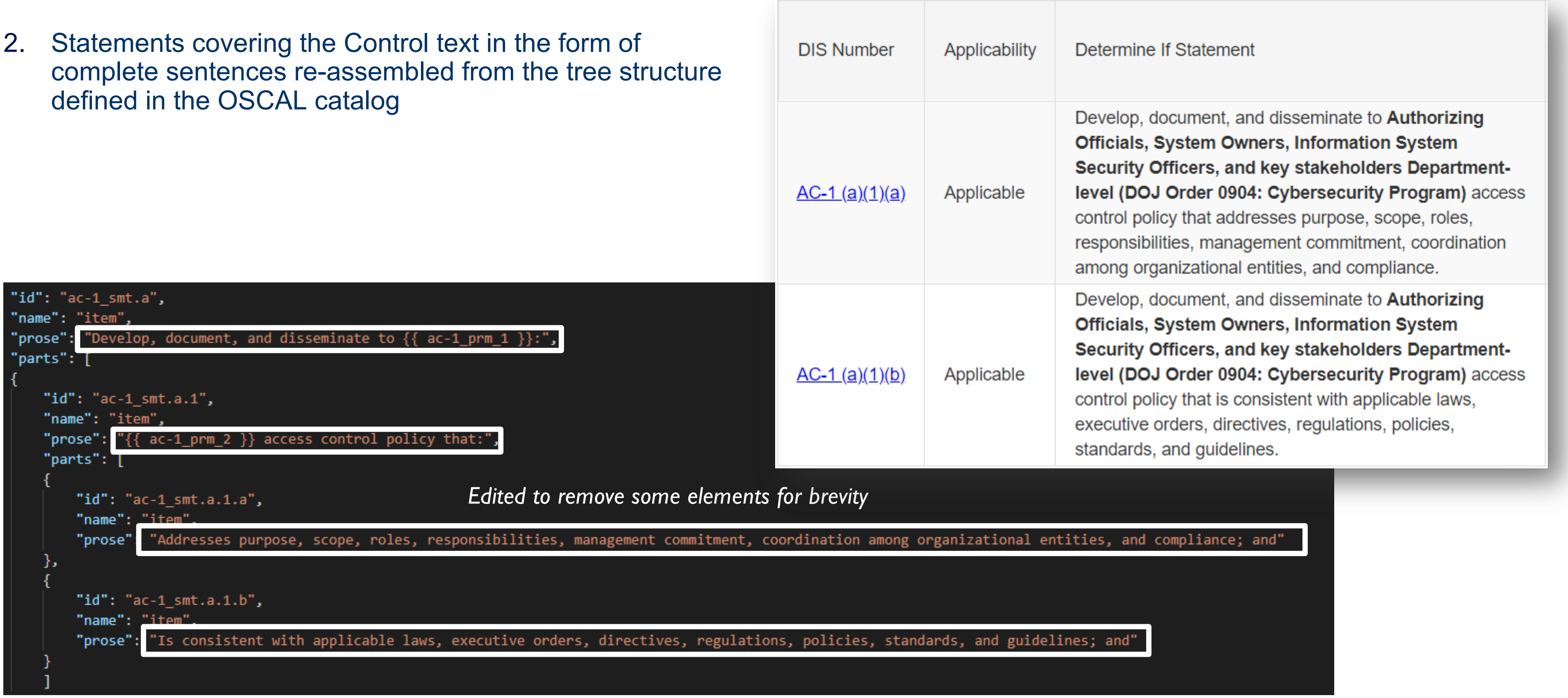
```
"params": [
    {
        "id": "ac-1_prm_1",
        "label": "organization-defined personnel or roles"
    },
```



DIS Number	Applicability	Determine If Statement
CPV-AC-1 [1]	Applicable	The following control parameter is defined: (P1) assignment: organization-defined personnel or roles

Interim Content Generated from OSCAL Catalog

2. Statements covering the Control text in the form of complete sentences re-assembled from the tree structure defined in the OSCAL catalog



DIS Number	Applicability	Determine If Statement
AC-1 (a)(1)(a)	Applicable	Develop, document, and disseminate to **Authorizing Officials, System Owners, Information System Security Officers, and key stakeholders Department-level (DOJ Order 0904: Cybersecurity Program)** access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
AC-1 (a)(1)(b)	Applicable	Develop, document, and disseminate to **Authorizing Officials, System Owners, Information System Security Officers, and key stakeholders Department-level (DOJ Order 0904: Cybersecurity Program)** access control policy that is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

```
"id": "ac-1_smt.a",
"name": "item",
"prose": "Develop, document, and disseminate to {{ ac-1_prm_1 }}:",
"parts": [
{
    "id": "ac-1_smt.a.1",
    "name": "item",
    "prose": "{{ ac-1_prm_2 }} access control policy that:",
    "parts": [
    {
        "id": "ac-1_smt.a.1.a",
        "name": "item",
        "prose": "Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and"
    },
    {
        "id": "ac-1_smt.a.1.b",
        "name": "item",
        "prose": "Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and"
    }
    ]
```

Edited to remove some elements for brevity

Publication of SP 800-53A, Revision 5

January 2022

- NIST publishes SP 800-53A, Revision 5 (Assessment Procedures)

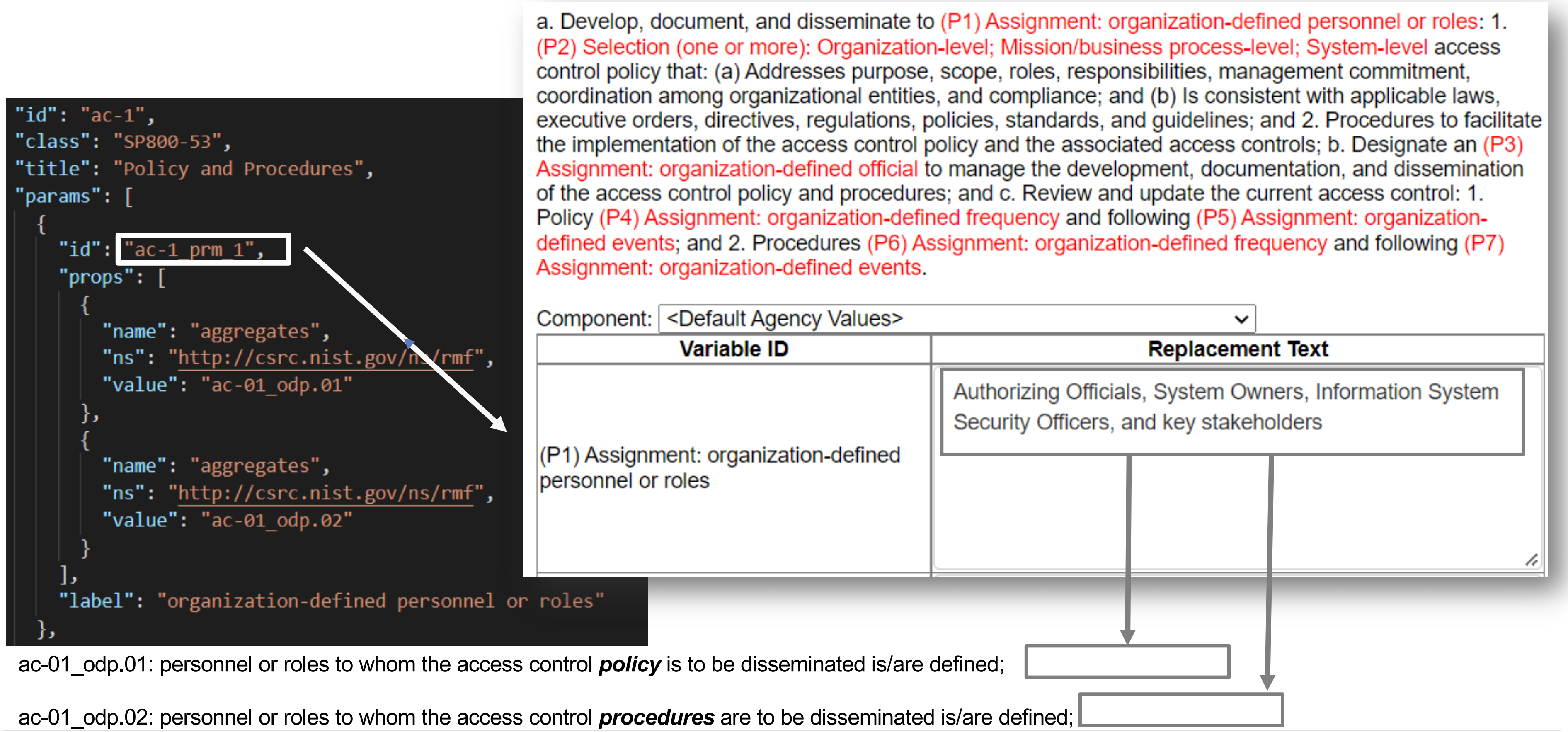
Current Work

- CSAM team is working with the updated OSCAL 800-53 Revision 5 catalog that incorporates the final 800-53A assessment procedures to generate the corresponding Determine If Statement content for CSAM.

Goals

- Update the NIST 800-53 Rev5 Control Set in CSAM with the final assessment procedures content to support future ingestion of OSCAL SAP and SAR data without losing any fidelity, e.g. have a home for every assessment result
- Support export of CSAM data in OSCAL with the same fidelity
- Provide customers already working with interim Rev5 content the ability to gradually migrate to final content over time
- Improve efficiency of CSAM User Interface for assessing more granular Determine If Statements
  - Interim NIST 800-53 Rev5 control set has 2,926 Determine If Statements
  - Final NIST 800-53 Rev5 control set will have 5,383 Determine If Statements (~84% increase)
- Handle the additional Control Parameters added within 800-53A in sensible manner for our customers by leveraging the OSCAL catalog's "aggregates" properties to map existing parameter values to the new more granular parameters added for 800-53A

Handling additional parameters added in 800-53A



```
"id": "ac-1",
"class": "SP800-53",
"title": "Policy and Procedures",
"params": [
  {
    "id": "ac-1_prm_1",
    "props": [
      {
        "name": "aggregates",
        "ns": "http://csrc.nist.gov/ns/rmf",
        "value": "ac-01_odp.01"
      },
      {
        "name": "aggregates",
        "ns": "http://csrc.nist.gov/ns/rmf",
        "value": "ac-01_odp.02"
      }
    ],
    "label": "organization-defined personnel or roles"
  },
```

a. Develop, document, and disseminate to (P1) Assignment: organization-defined personnel or roles: 1. (P2) Selection (one or more): Organization-level; Mission/business process-level; System-level access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an (P3) Assignment: organization-defined official to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy (P4) Assignment: organization-defined frequency and following (P5) Assignment: organization-defined events; and 2. Procedures (P6) Assignment: organization-defined frequency and following (P7) Assignment: organization-defined events.

Component: <Default Agency Values>

Variable ID	Replacement Text
(P1) Assignment: organization-defined personnel or roles	Authorizing Officials, System Owners, Information System Security Officers, and key stakeholders

ac-01_odp.01: personnel or roles to whom the access control ***policy*** is to be disseminated is/are defined;

ac-01_odp.02: personnel or roles to whom the access control ***procedures*** are to be disseminated is/are defined;

DOJ Cyber Security Points of Contact

POC	Contact Information
Vu Nguyen Chief Information Security Officer (Acting) Office of the Chief Information Officer Department of Justice	Vu.Nguyen@usdoj.gov (202) 532-5364
Ramon Burks Assistant Director Engineering & ICAM Office of the Chief Information Officer Department of Justice	Ramon.Burks@usdoj.gov (202) 598-9426
Daphna Shai Shared Cybersecurity Services Program Manager Cybersecurity Services Staff Office of the Chief Information Officer Department of Justice	Daphna.shai@usdoj.gov (202) 616-0768
Samantha Hoang CSAM Federal Lead Cybersecurity Services Staff Office of the Chief Information Officer Department of Justice	Samantha.Hoang@usdoj.gov 202-598-3371
Ritul Walia Client Engagement Manager Office of the Chief Information Officer Department of Justice	Ritul.Walia@usdoj.gov (202) 616-1490