NREL
Transforming ENERGY

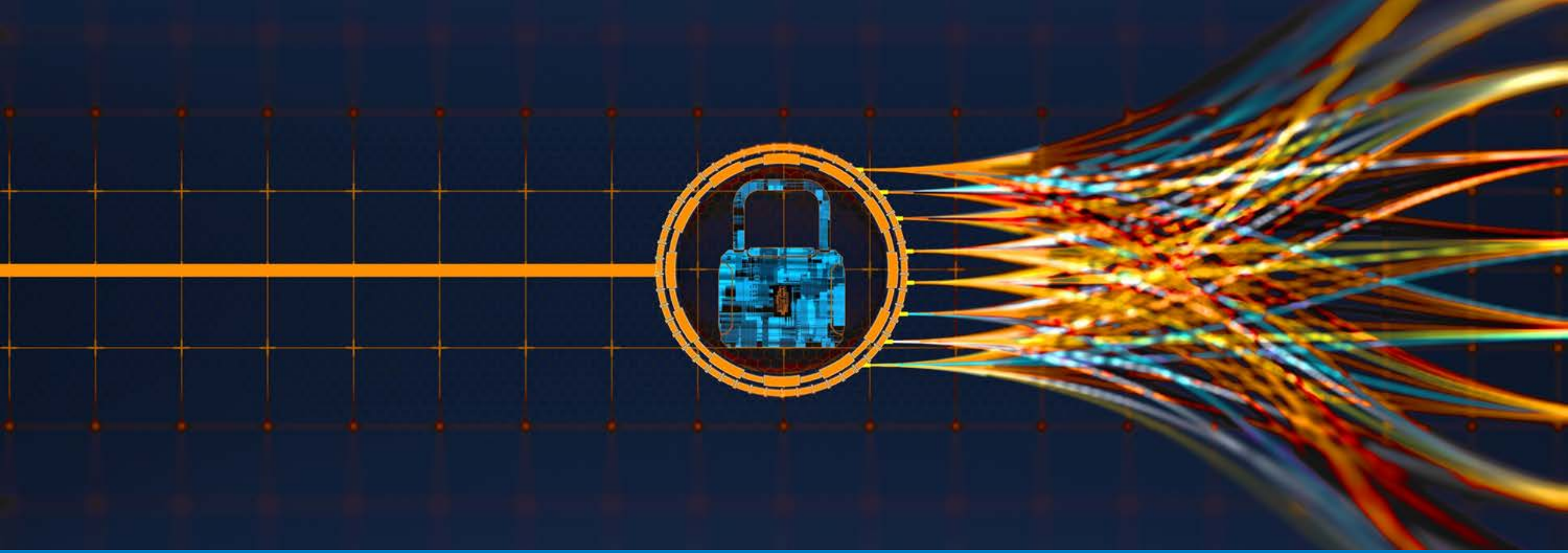
Automation for Distributed Energy Resources Risk Manager using OSCAL

Anuj Sanghvi
Cybersecurity Research Engineer
Paul Wand
Cybersecurity Visualization Engineer

Cybersecurity for Distributed Energy Resources

Modern energy systems are increasingly reliant on smaller decentralized generation sources, i.e., **distributed energy resources (DERs)** such as solar, wind, and storage.

- DERs use multiple separate communications networks to connect with the energy grid.
- This growing number of smart devices that support DERs can increase the number of access points outside a utility's administrative domain, which can increase the potential for cyber vulnerabilities and limit utility visibility over the entire system.



The Distributed Energy Resources Cybersecurity Framework (DERCF) was developed to help federal agencies mitigate gaps in their cybersecurity posture for distributed energy systems.

The Distributed Energy Resources Risk Manager

- NREL extended the scope of the DERCF to include the NIST Risk Management Framework (RMF), addressing the challenges faced by federal energy managers when complying with the NIST RMF for DER systems
- The NIST RMF is a cyclical process designed to incorporate principles of security and risk management into an organization's system policies and procedures.
- As an additional tool, NREL's **Distributed Energy Resources Risk Manager (DER-RM)** is independent of the DERCF's existing self-assessment and allows users to focus on the RMF process.

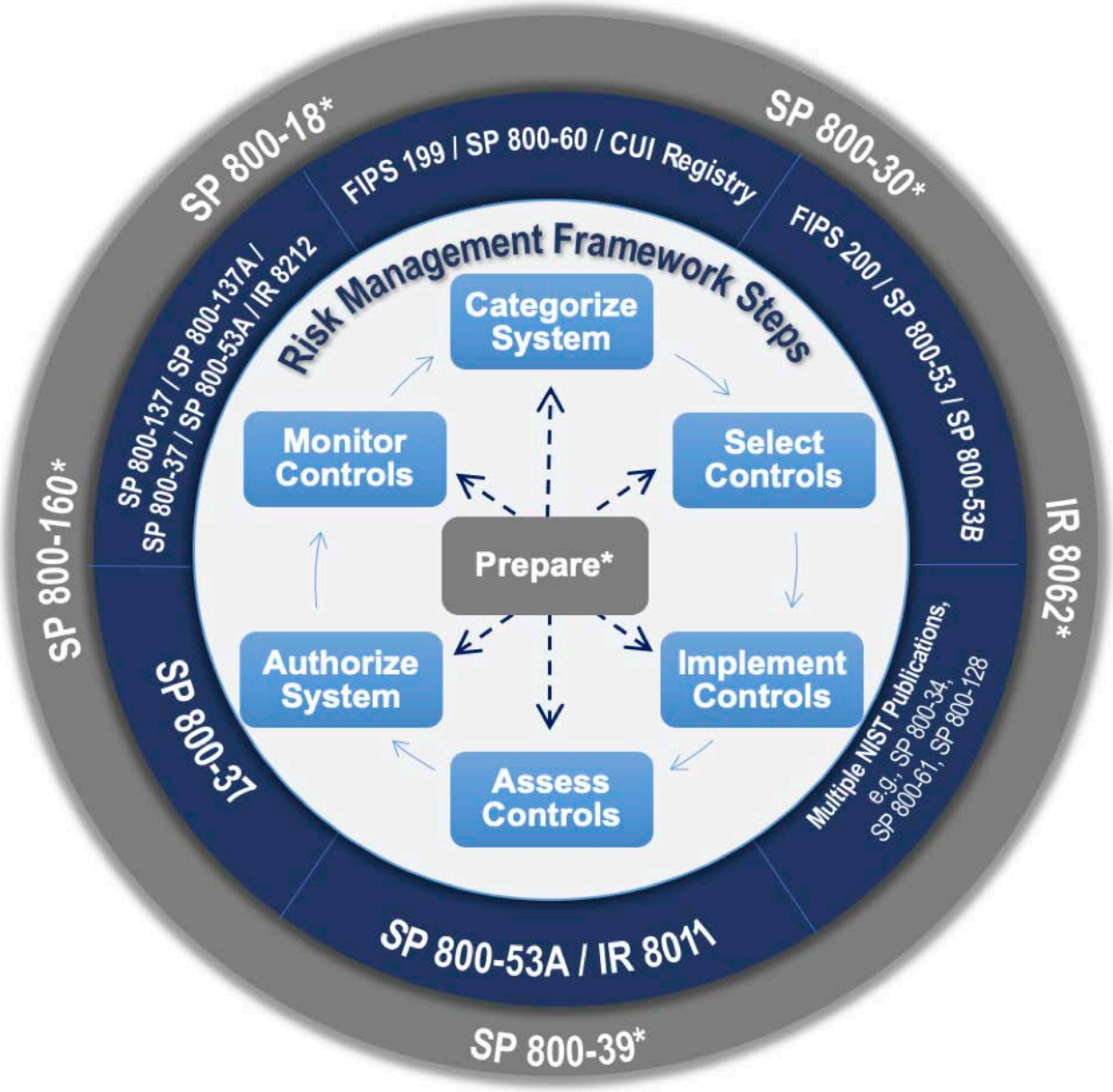


Illustration from NIST

DER-RM Goals

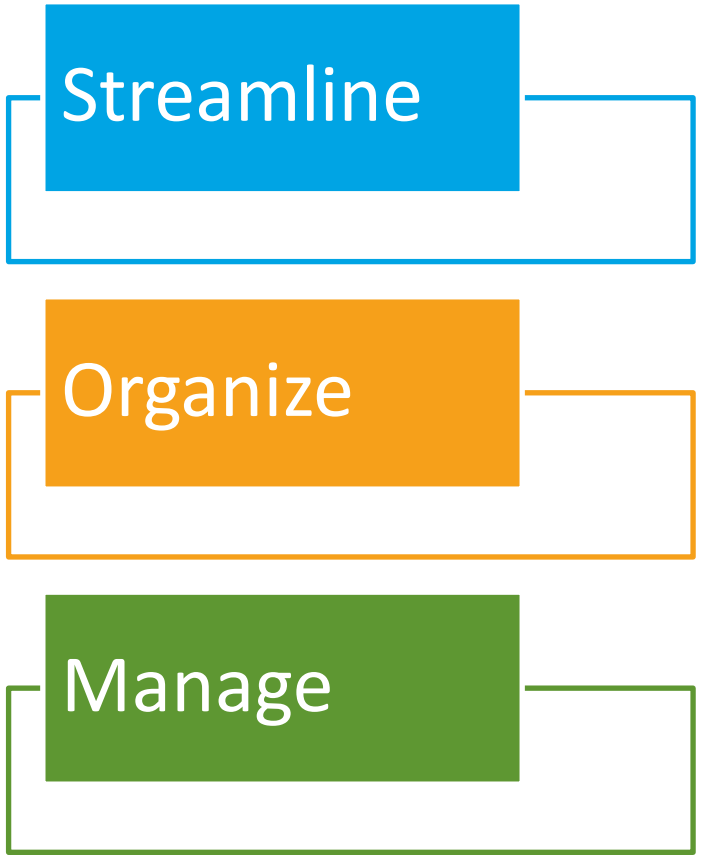
- **Navigate compliance**

  Manage cybersecurity risk with government requirements in an organized manner
- **Automate requirements**

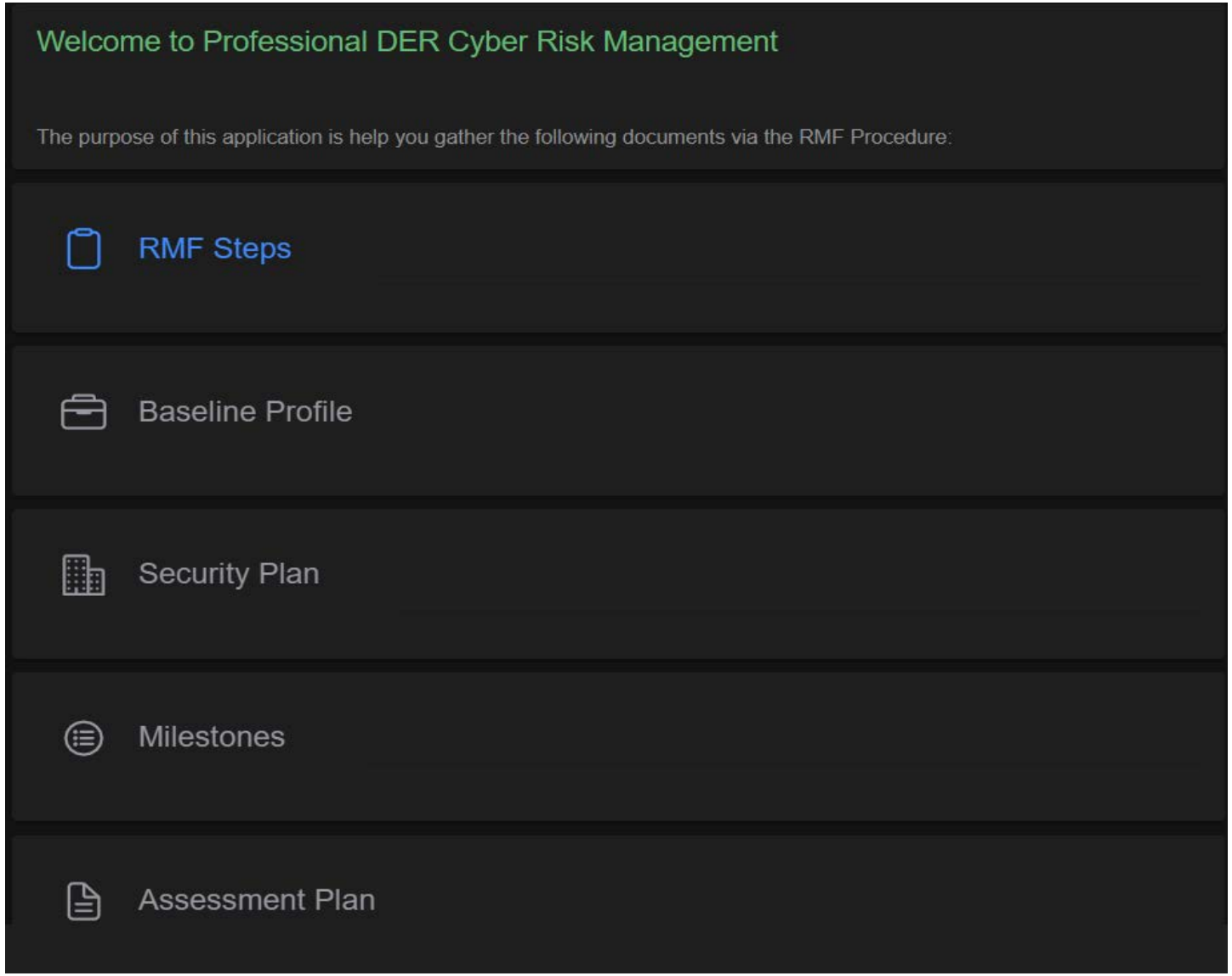
  Adapt to specific organization needs and present the most aligned templates and recommendations
- **Provide knowledge**

  Apply NIST guidance and DER-RM specific approaches
- **User-friendly interaction**

  Calculate risk score and generate system-specific requirements through real-world examples



DER-RM Prototype



Discovering OSCAL

nist.gov/publications/search?k=rmf&d%5Bmin%5D=&d%5Bmax%5D=&t=&a=&s=All&n=

cs CyberSecurity/oscal...

An official website of the United States government Here's how you know

NIST

Search NIST

Menu

Publications

Search

rmf

Search Title, Abstract, Conference, Citation, Keyword or Author

Published date

From

And

To

Advanced search +

NIST Authors in **Bold**

Displaying 1 - 8 of 8

A Document-based View of the Risk Management Framework

AUGUST 3, 2020

AUTHOR(S): JOSHUA LUBELL

Cybersecurity professionals know the Risk Management Framework as a rigorous yet flexible process for managing security risk. But the RMF lacks a document focus

The Next Generation Risk Management Framework (RMF 2.0): A Holistic Methodology to Manage Information Security, Privacy and Supply Chain Risk

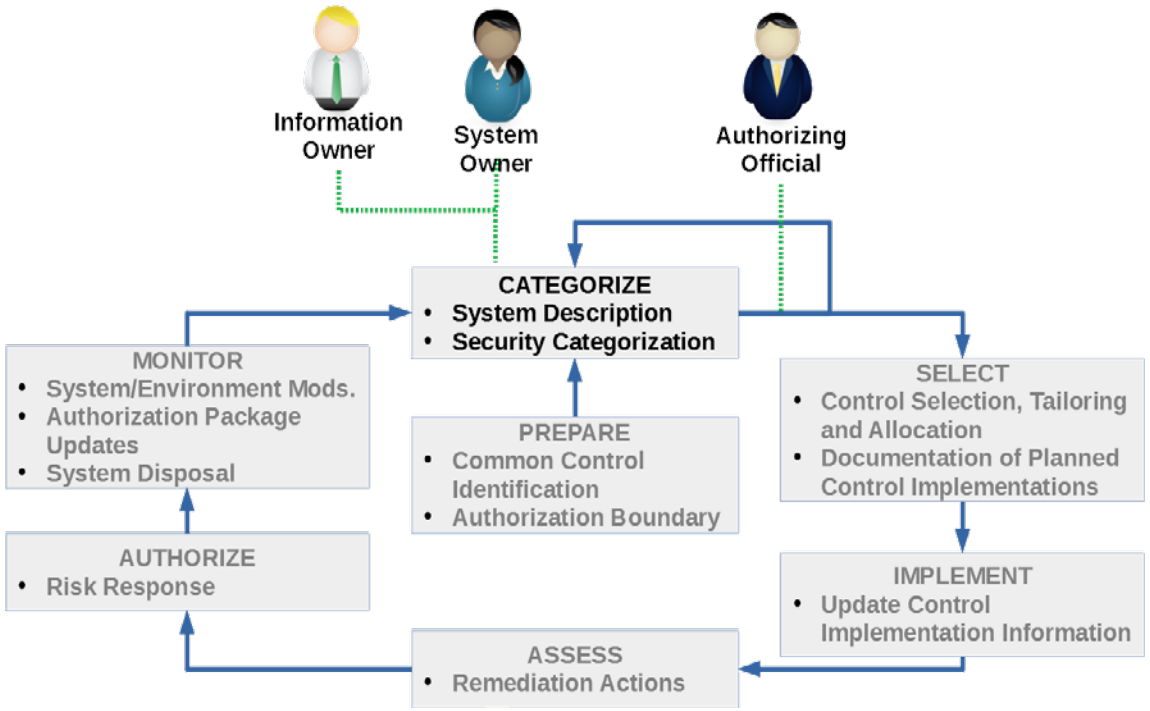
FEBRUARY 28, 2019

AUTHOR(S): VICTORIA Y. PILLITTERI

This bulletin summarizes the information found in NIST SP 800-37, Revision 2: Risk Management Framework for Information Systems and Organizations: A System Life

The Link Between OSCAL & RMF

A document-based view of the RMF



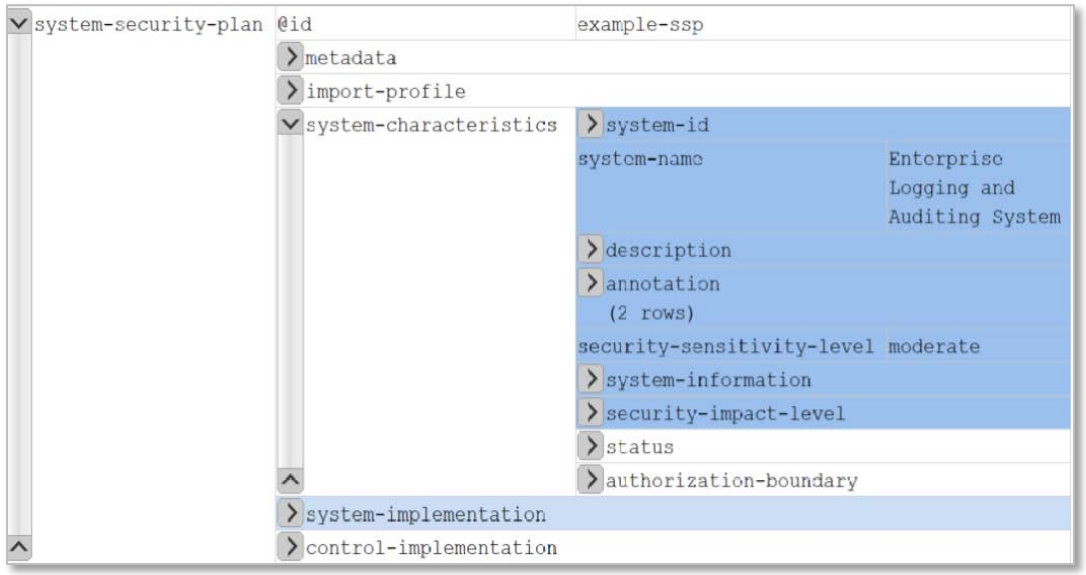


Illustration from NIST

The Layers of OSCAL

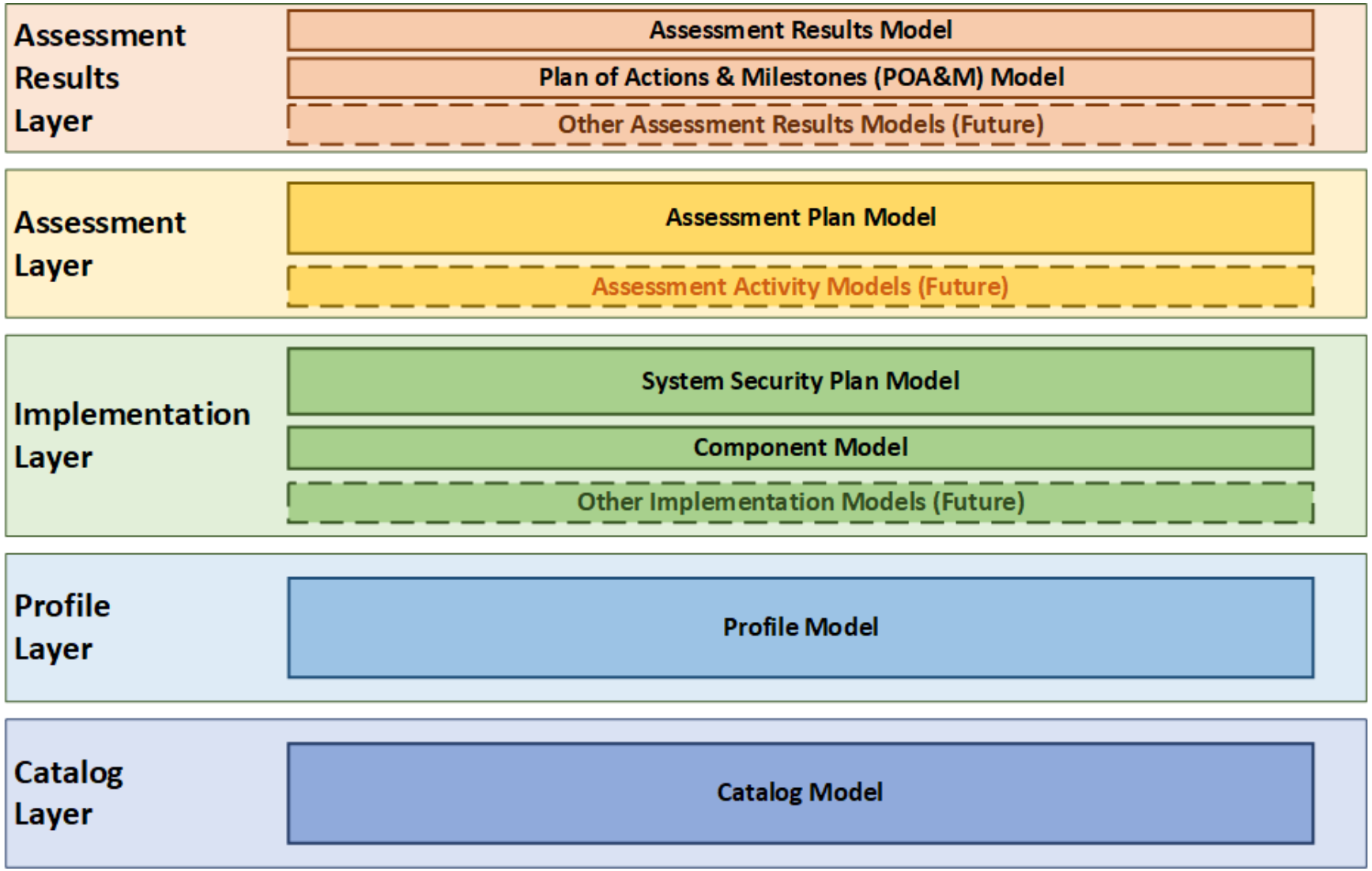


Illustration from NIST

The Extensible Nature of OSCAL

And why OSCAL is good for automation

Annotated Property

An attribute, characteristic, or quality of the containing object expressed as a namespace qualified name/value pair with optional explanatory remarks. The value of an annotated property is a simple scalar value.

```
▼ object {1}
  ▼ annotations [2]
    ▼ 0 {2}
        name : deployment-model
        value : private
    ▼ 1 {2}
        name : service-models
        value : iaas
```

The Extensible Nature of OSCAL

And why OSCAL is good for automation

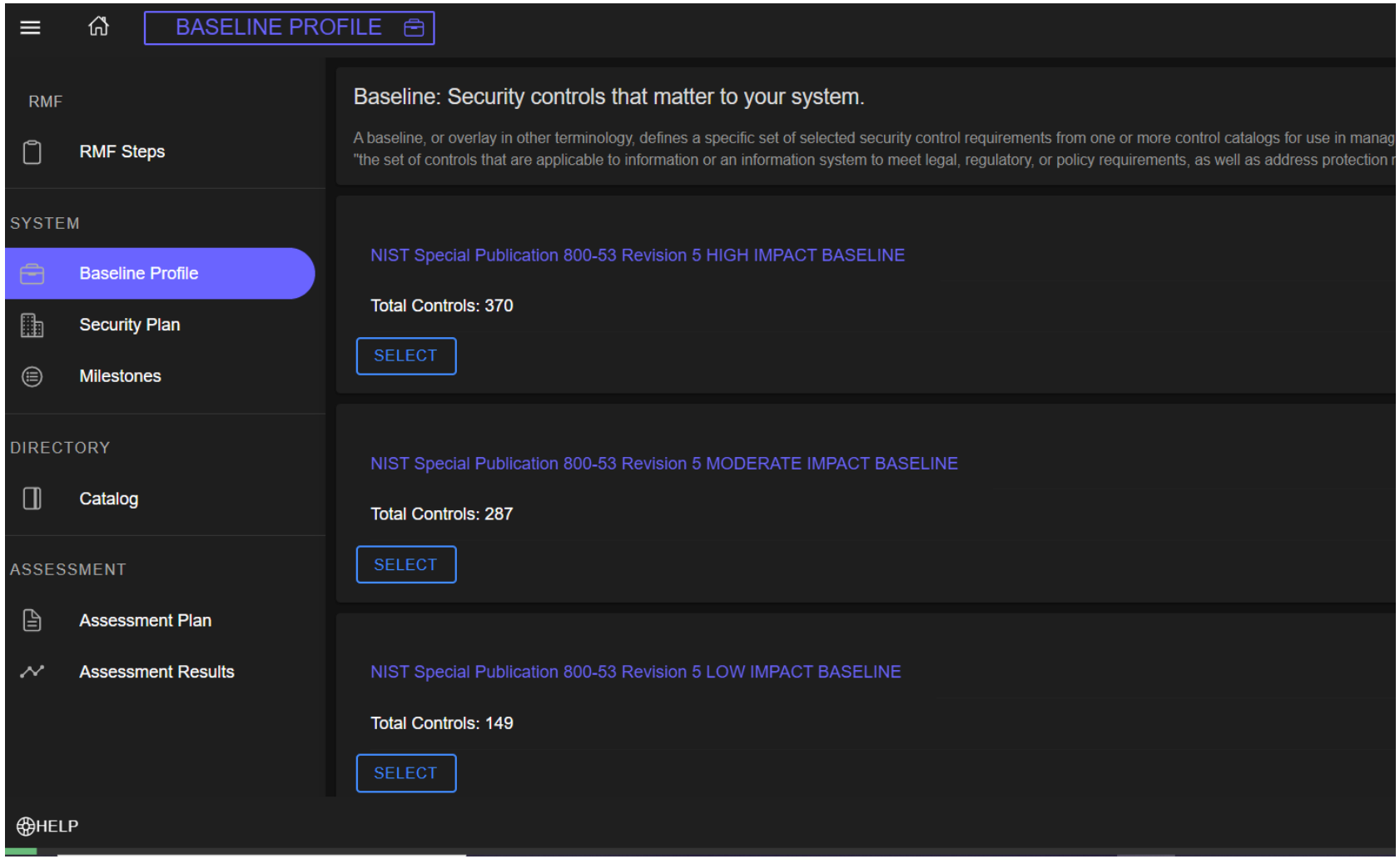
FedRAMP Specific Examples

FedRAMP Information		All FedRAMP Compliance tags must use name='conformi ns='https://fedramp.gov/ns/oscal'
Data	**Tag Value**	**Placement as deisgnated by XPath Notation**
Test Case Workbook Objective	assessment-objective	**/*/modify/alter/add**
Data Center	data-center	**/*/metadata/location**
Primary Data Center	primary-data-center	**/*/metadata/location**
Backup or Alternate Data Center(s)	alternate-data-center	**/*/metadata/location**
FIPS 140-2 Validated Component	fips-140-2-validated	**/*/system-implementation/component**
False Positive Details	false-positive	**/*/results/finding/observation**
Operational Requirement Details	operationally-required	**/*/results/finding/observation**
Risk Adjustment Details	risk-adjustment	**/*/results/finding/observation**

Source: https://github.com/GSA/fedramp-automation/blob/master/documents/FedRAMP_OSCAL_Registry.xlsx

Custom NREL Baselines for DER

Assessment results layer



Control Catalog

CATALOG

NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations

Control Group Families

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection

Configuration Management

- Configuration Management Policy and Procedures
- Baseline Configuration
- Configuration Change Control
- Security Impact Analysis
- Access Restrictions for Change
- Configuration Settings
- Least Functionality
- Information System Component Inventory
- Configuration Management Plan
- Software Usage Restrictions
- User-installed Software

Baseline Configuration

ADD TO BASELINE | IMPLEMENT CONTROL

Statement

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Guidance

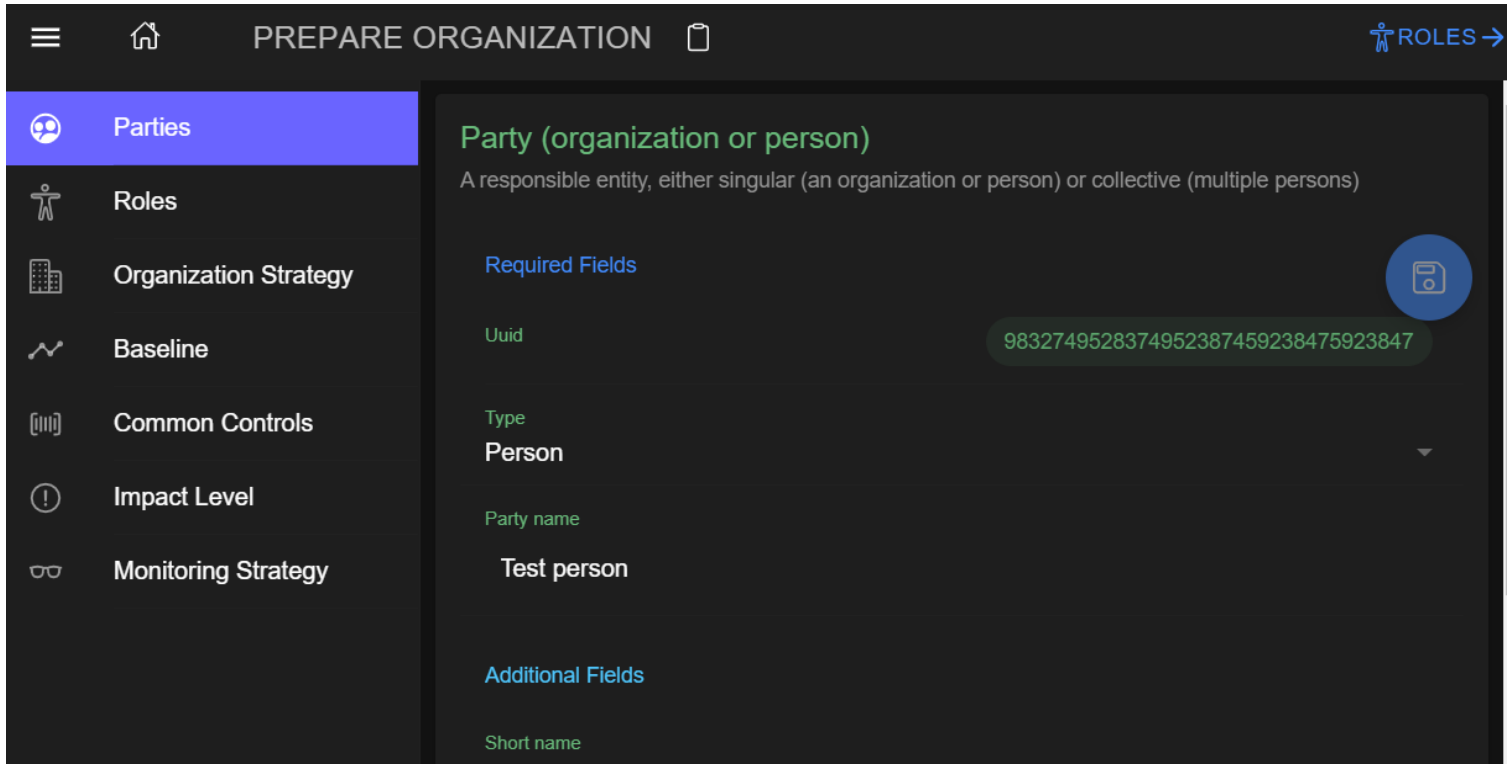
This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.

Objective

Determine if the organization:

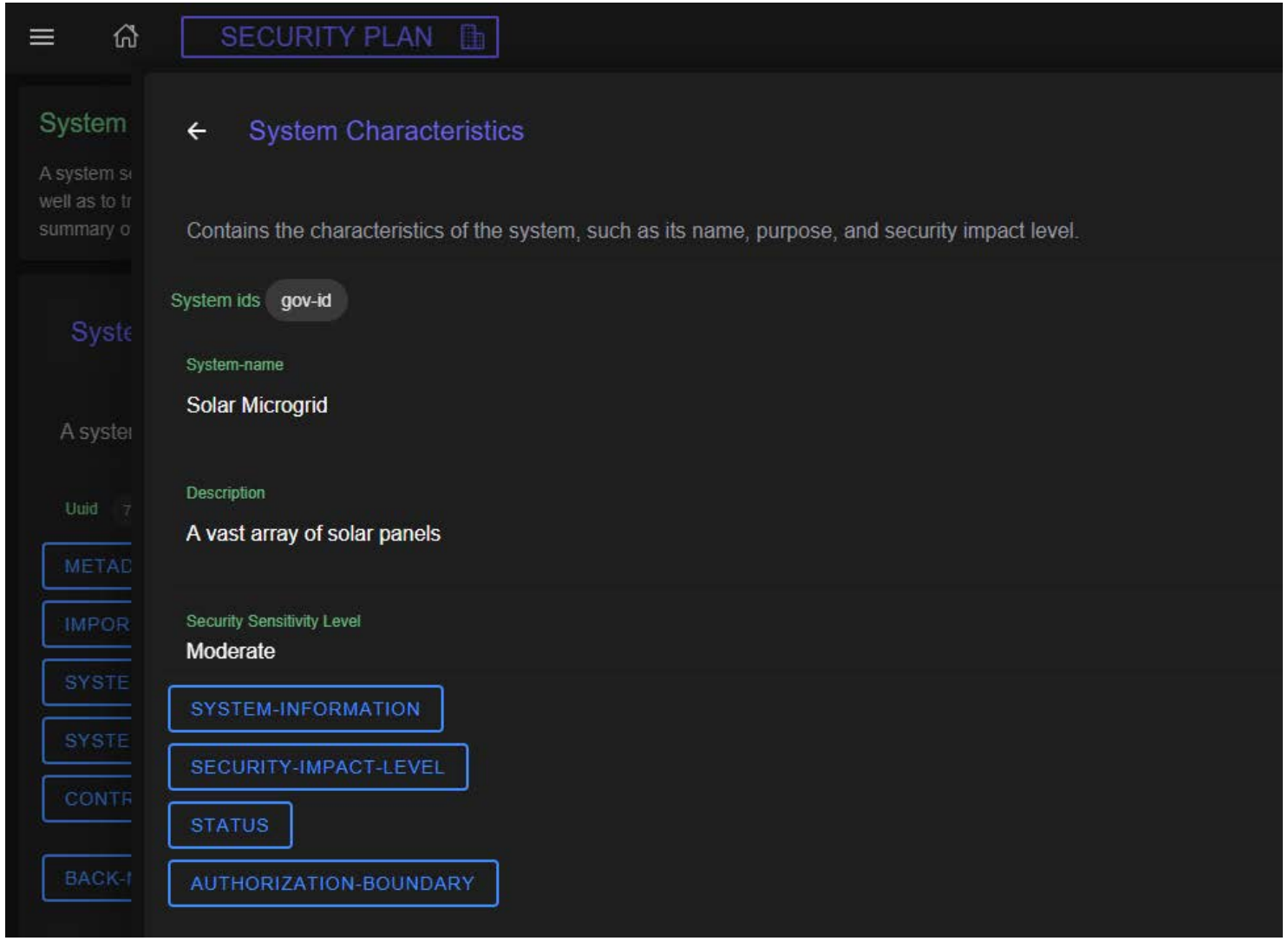
OSCAL Input

Accepts forms for manual entry and a JSON endpoint for automation



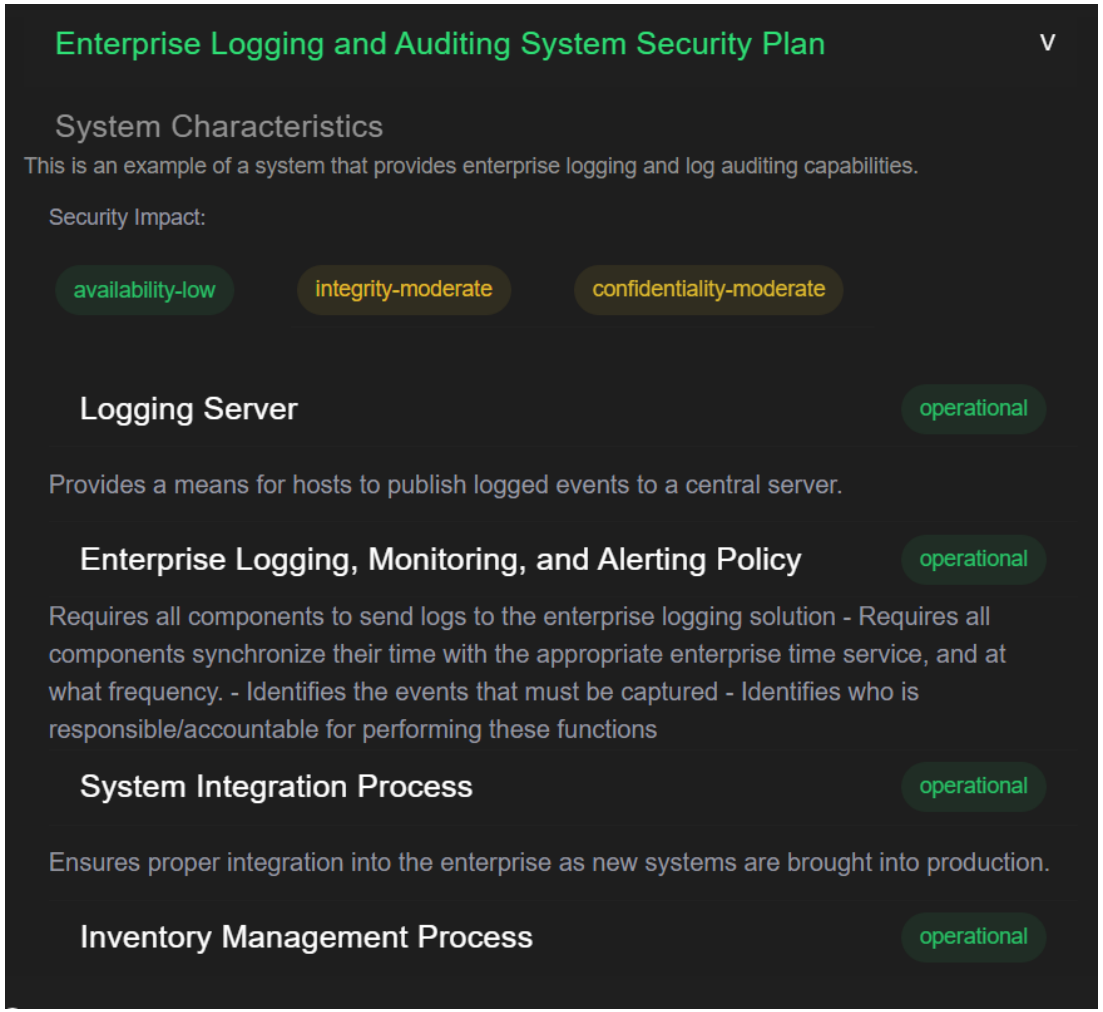
OSCAL Input

Accepts forms for manual entry and a JSON endpoint for automation



OSCAL Output

Exports PDF and OSCAL JSON



Source: https://pages.nist.gov/OSCAL/documentation/schema/

Automated Continuous Monitoring

Assessment results layer

Globals / RiskLogEntry /

Interface RiskLogEntry

Identifies the result of an action and/or task that occured as part of executing an assessment plan or an assessment event that occured in producing the assessment results. Identifies the result of an action and/or task that occured as part of executing an assessment plan or an assessment event that occured in producing the assessment results.

Hierarchy

- **RiskLogEntry**

Index

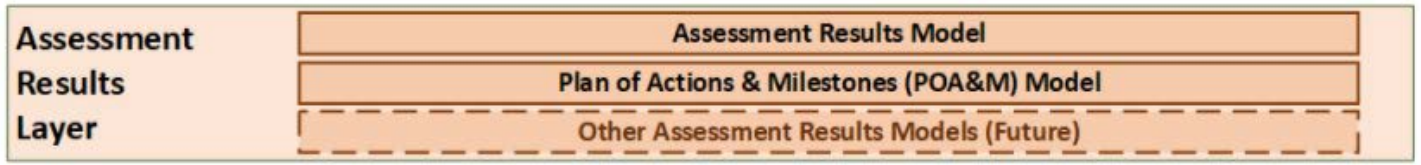
Properties

annotations	logged_by	start
description	props	status_change
end	related_responses	title
links	remarks	uuid

Properties

Globals

RiskLogEntry
- annotations
- description
- end
- links
- logged_by
- props
- related_responses
- remarks
- start
- status_change
- title
- uuid



Automated Continuous Monitoring

Assessment results layer

RiskLogEntryUniversallyUniqueIdentifier

T `RiskLogEntryUniversallyUniqueIdentifier: string`

Defined in src/poam/index.ts:214

Uniquely identifies an assessment event. This UUID may be referenced elsewhere in an OSCAL document when refering to this information. A UUID should be consistantly used for this schedule across revisions of the document.

RiskResolutionDeadline

T `RiskResolutionDeadline: string`

Defined in src/poam/index.ts:188

The date/time by which the risk must be resolved.

RiskStatement

T `RiskStatement: string`

Defined in src/shared/IdentifiedRisk.ts:36
Defined in src/poam/index.ts:148

An summary of impact for how the risk affects the system. An summary of impact for how the risk affects the system.

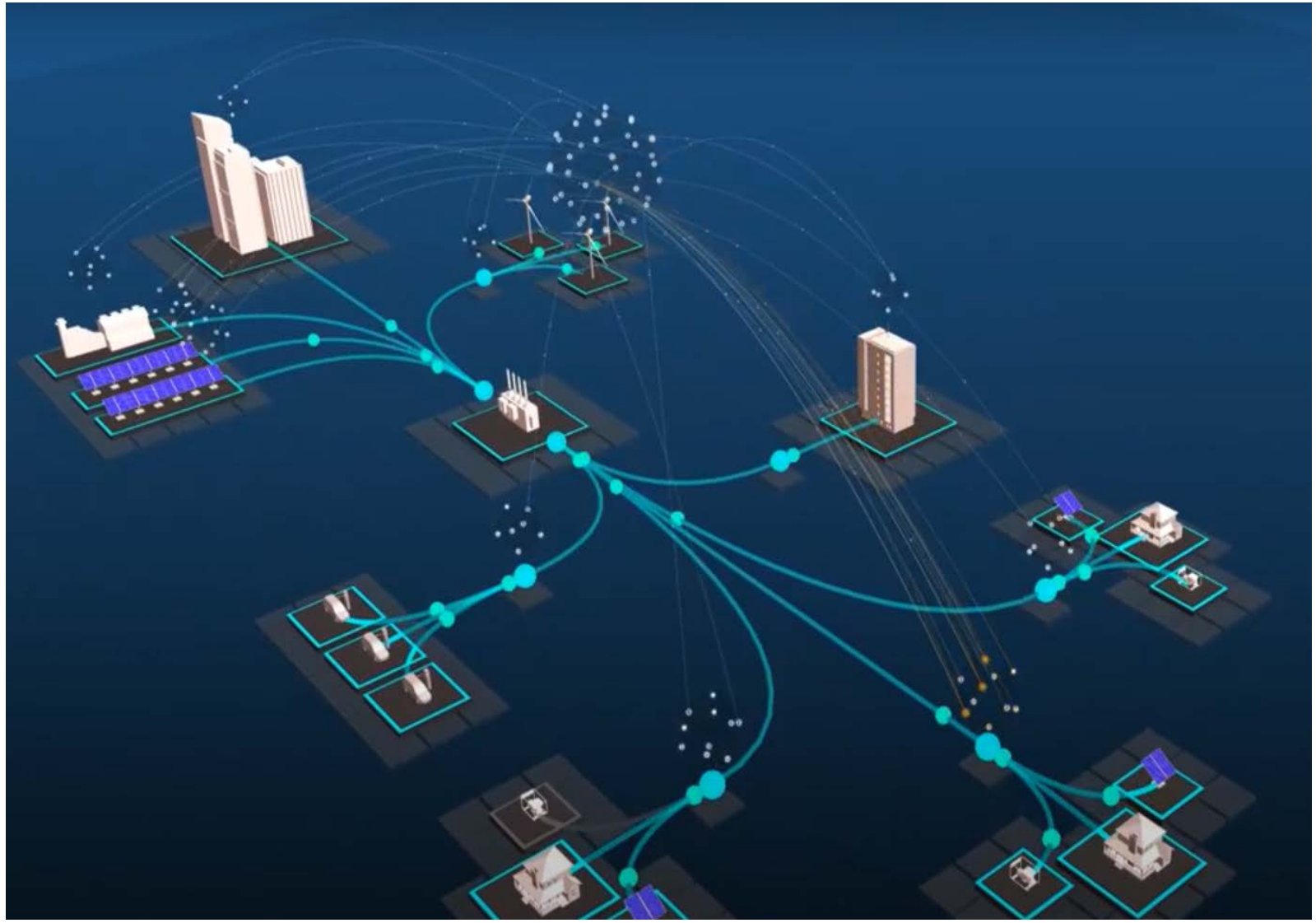
RiskStatus

T `RiskStatus: string`

Defined in src/poam/index.ts:226

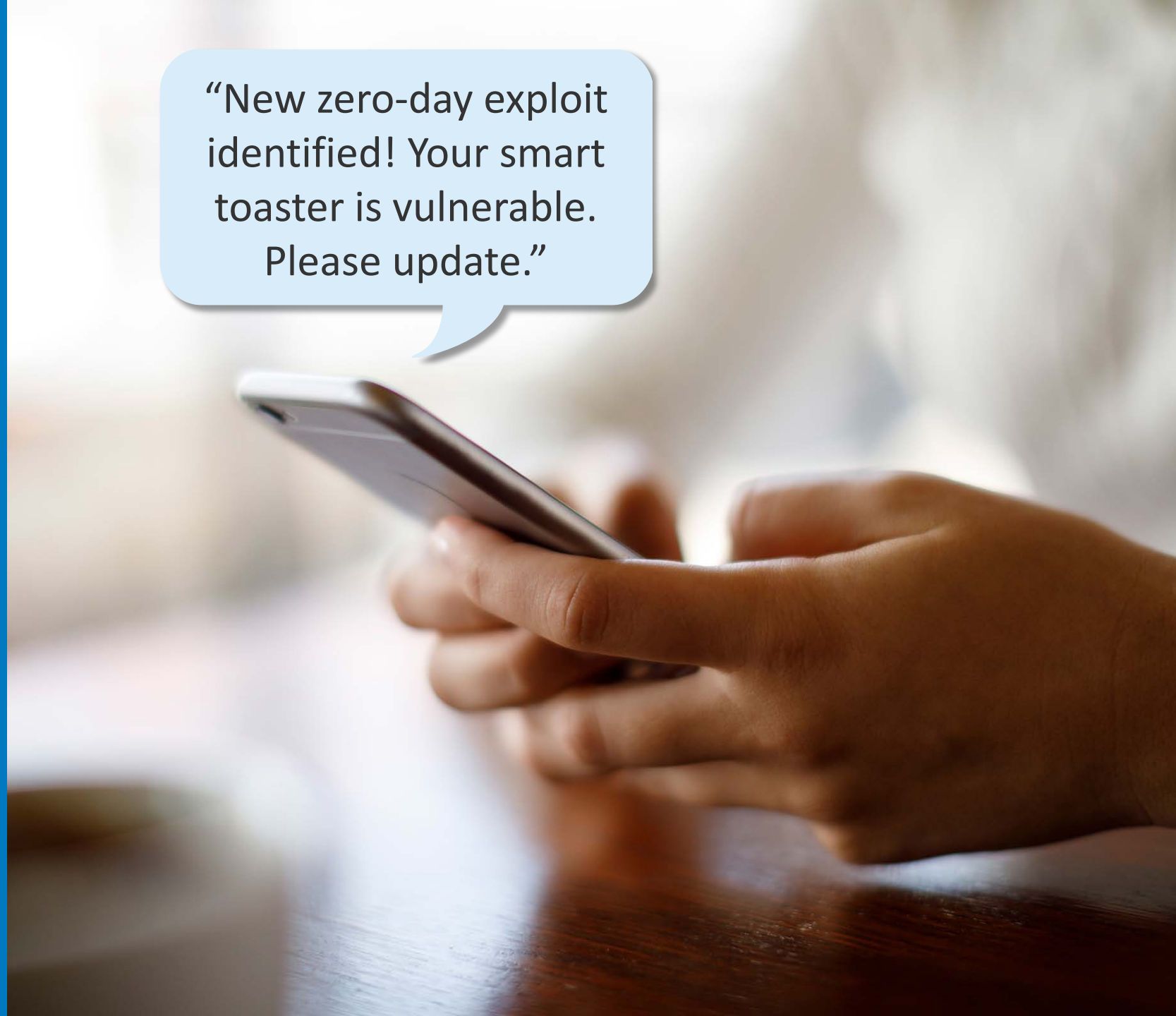
Describes the status of the associated risk.

Connecting OSCAL to Network Monitoring Solution



Automating Risk Awareness

Combine automated security scanning with OSCAL to send notifications directly to the responsible parties for system components violating security controls



Q&A

NREL/PR-5R00-78942

www.nrel.gov

Contact:
Tami Reynolds – Tami.Reynolds@nrel.gov
Anuj Sanghvi – Anuj.Sanghvi@nrel.gov
Paul Wand – Paul.Wand@nrel.gov

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Federal Energy Management Program Office. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

NREL
Transforming ENERGY