



Facility-Related Control System RMF Self-Assessment Tool R-SAT

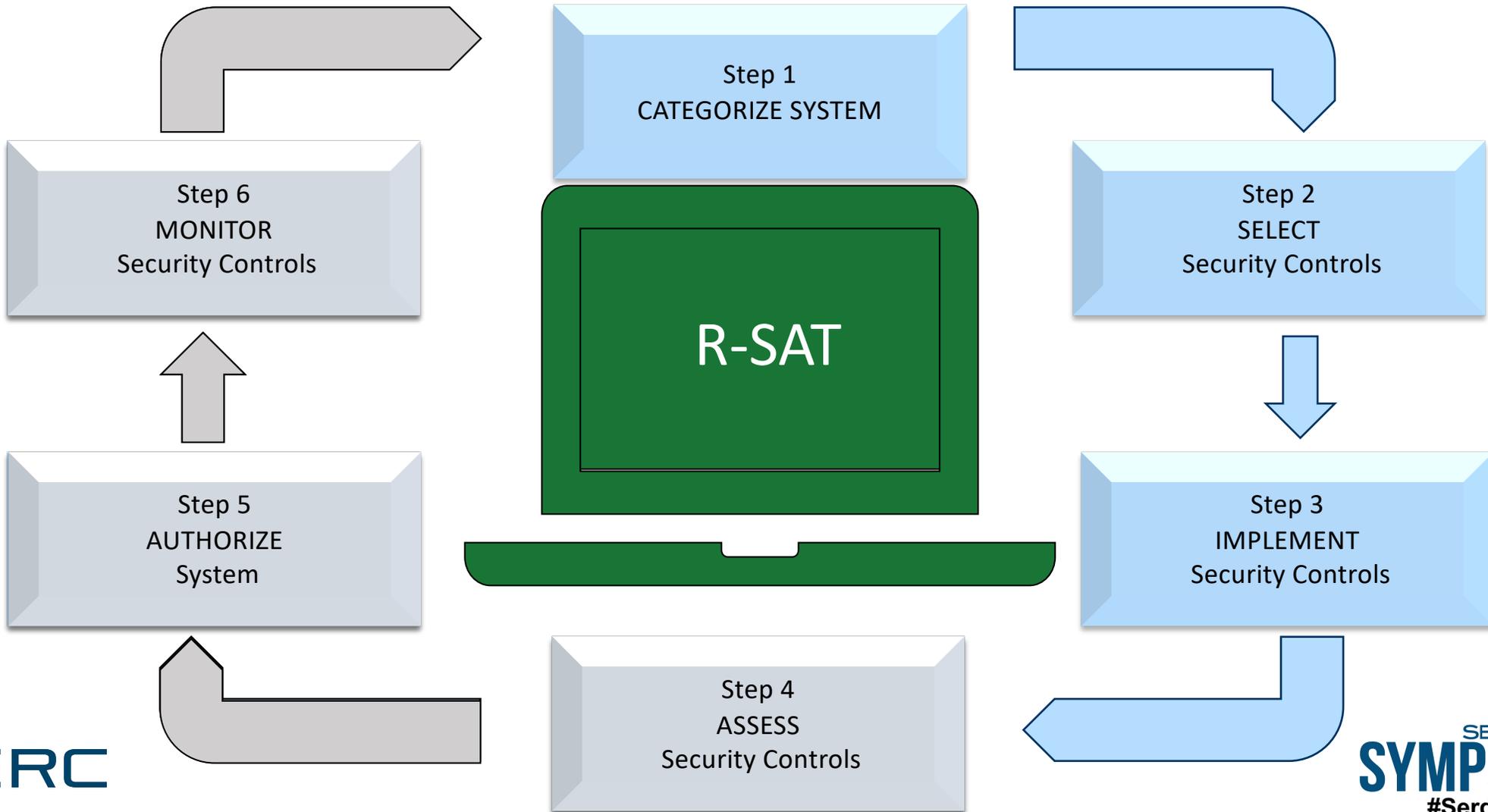
Aura Lee Keating

IPERC



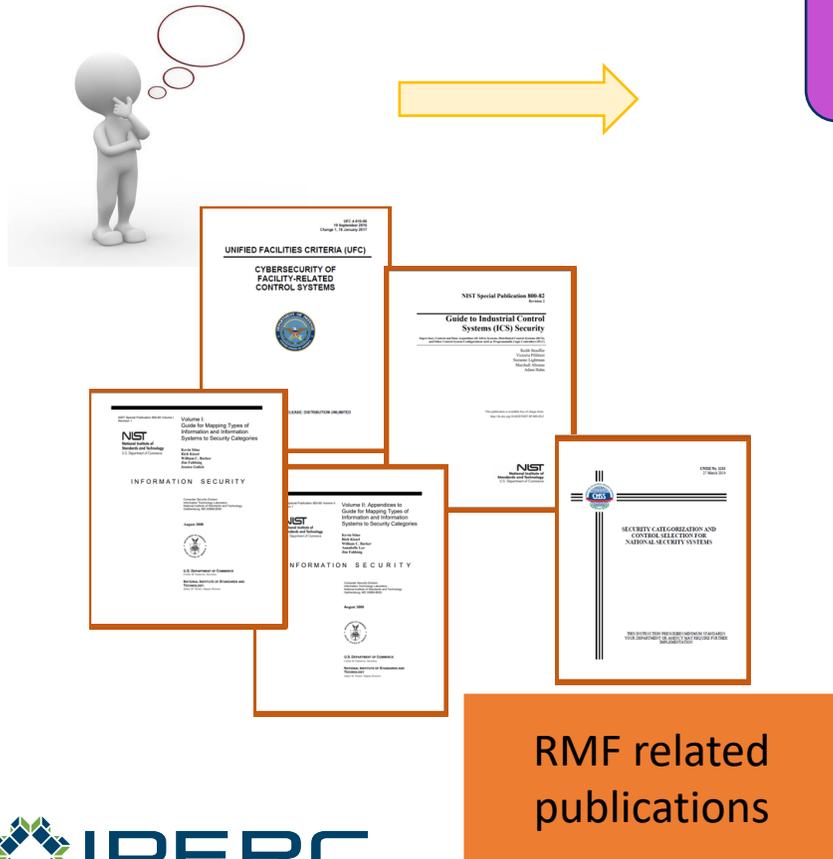
SERDP • ESTCP
SYMPOSIUM
2019 | Enhancing DoD's Mission Effectiveness

RMF Self Assessment Process

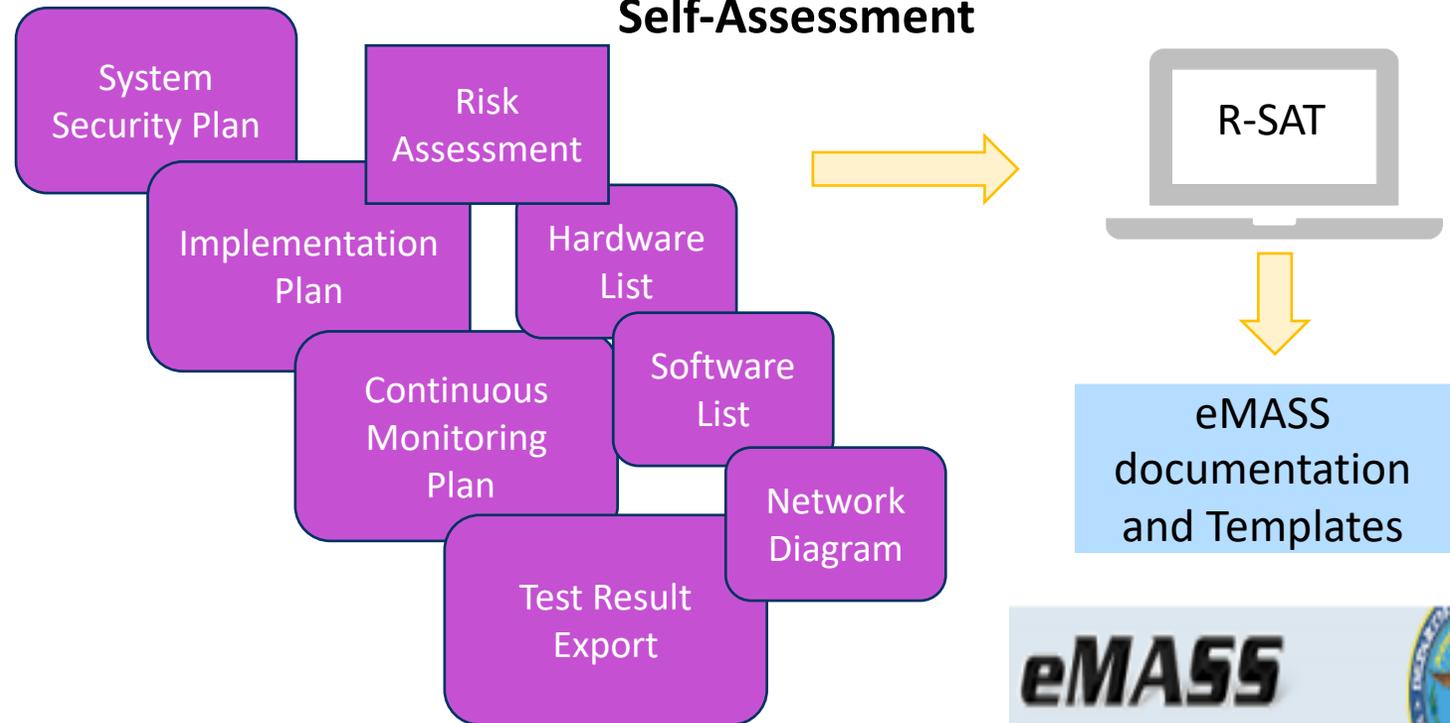


FRCS RMF Self-Assessment Tool (R-SAT)

The RMF Process can be overwhelming for System Owners



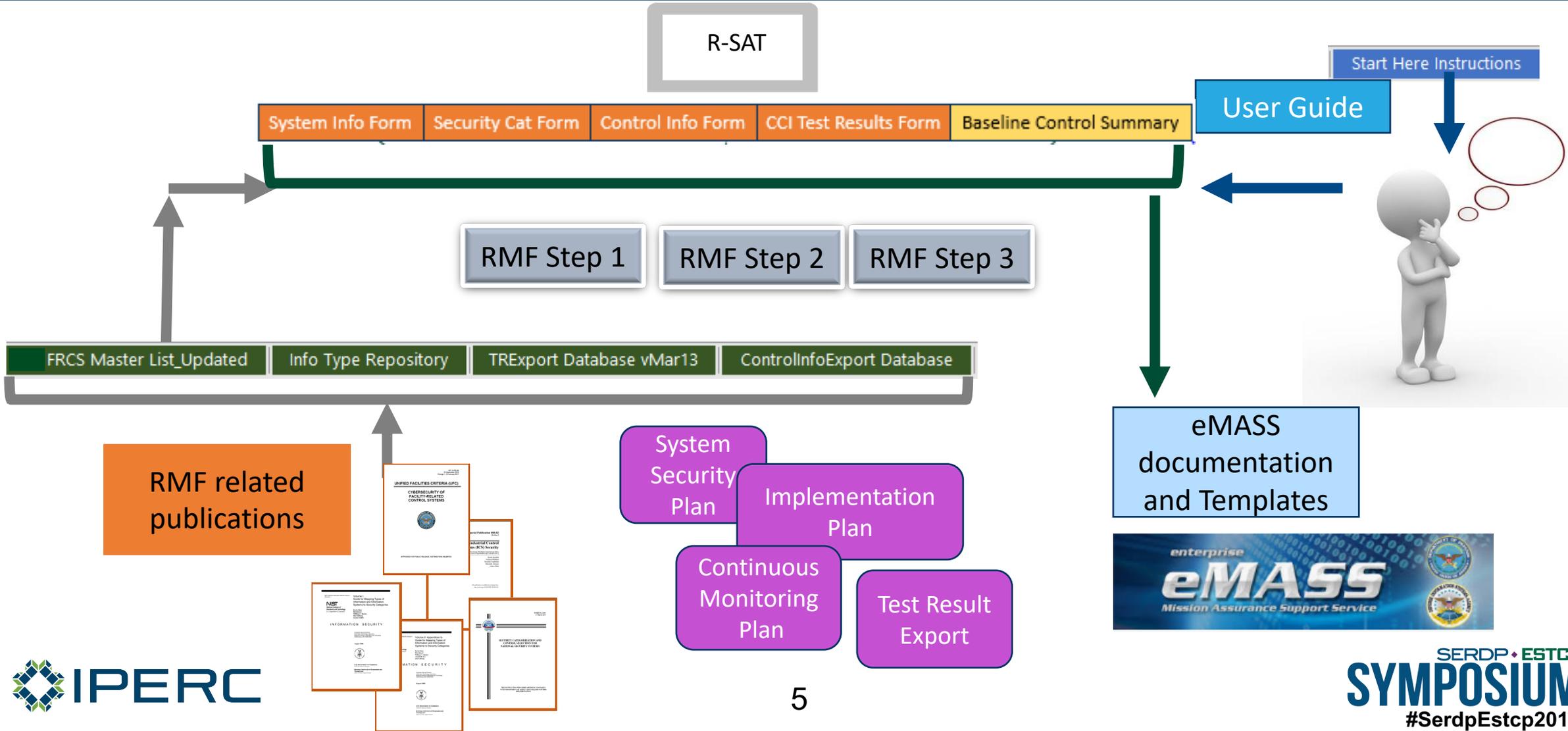
A resource to aid System Owners with RMF Self-Assessment



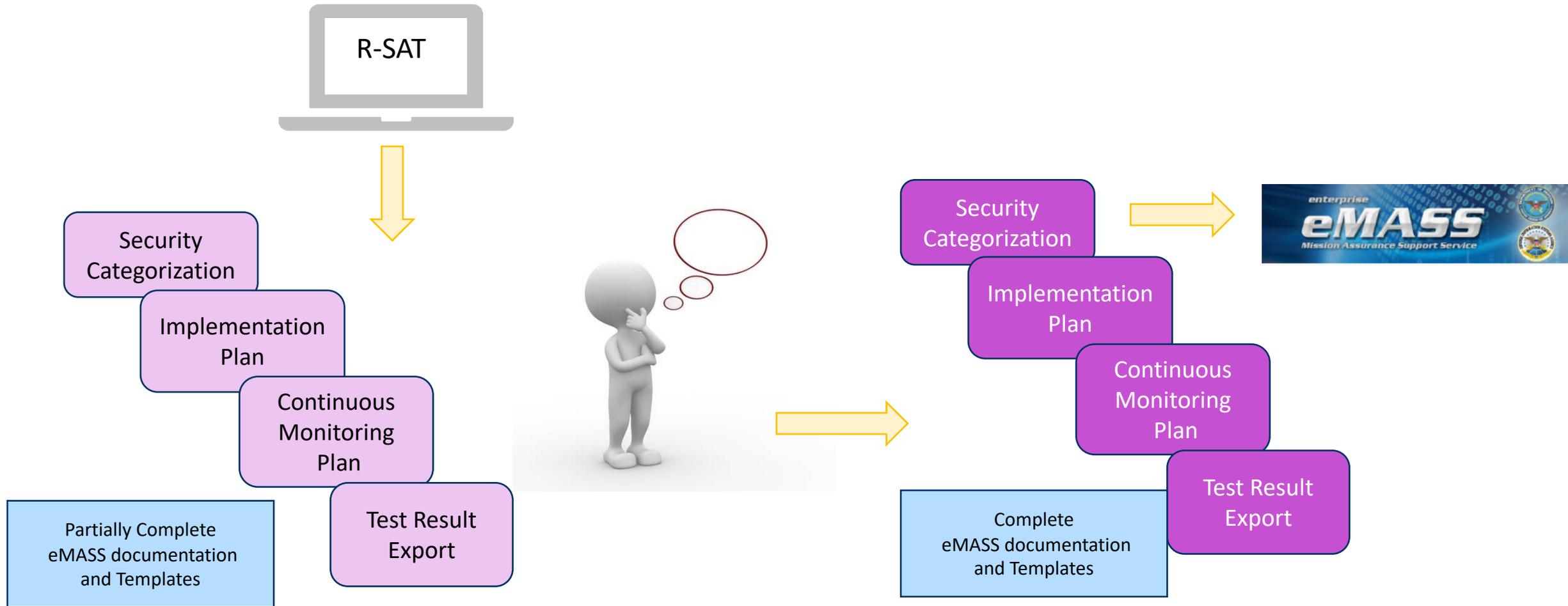
R-SAT Overview



R-SAT Process



R-SAT Outputs

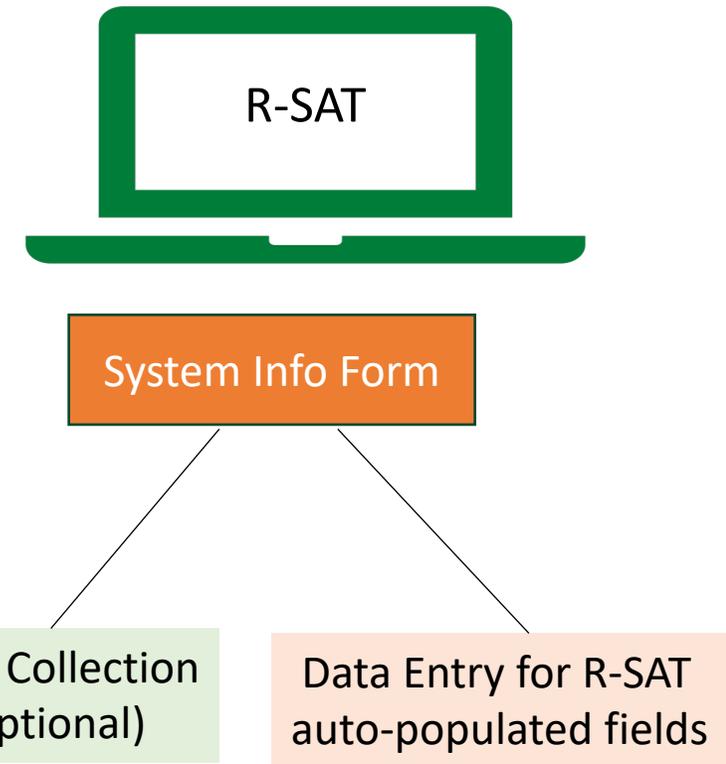


Step 0 – Register System in eMASS

Step 0
System Registration

Acronym	Version	Authorization Status
TEST MC4800-CS-PE-I-AA	Control System Platform Enclave (PE)	Not Yet Authorized
TEST MC4800-CS-UCS-NI-A	Utility Control System (UCS)	Not Yet Authorized
TEST MC4800-CS-BCS-I-AA	Building Control System (BCS)	Not Yet Authorized
TEST MC4800-CS-FLS-NI-A	Fire & Life Safety System (FLS)	Not Yet Authorized
TEST MC4800-CS-ESS-NI-A	Electronic Security System (ESS)	Not Yet Authorized

eMASS Home Screen



Step 2 – Select Controls

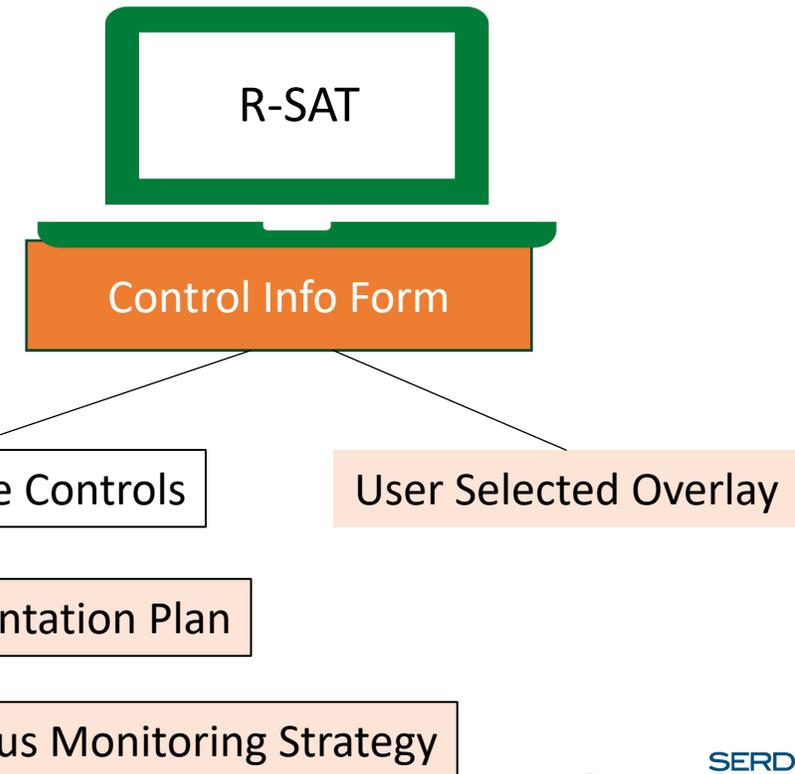
Step 2
SELECT
Security Controls

Baseline Controls based on CNSSI 1253

User option for applying overlay to tailor population of form

Populated standard responses to template fields

Control Information Form															
Control Information			Implementation Plan						IM	SLCM					
Control	Control Title	Control Description	Implementa	Common	Security	N/A	Estimated	Comments	Responsible	Criticality	Frequency	Method	Reporting	Tracking	SLCM
AC-1	Access Control	Description:	Planned							CRW/G White					
AC-2	Account	Description:	Planned							CRW/G Yellow					
AC-2(1)	Automated	Description:	Planned							CRW/G White					
AC-2(2)	Removal Of	Description:	Planned							CRW/G White					
AC-2(3)	Disable	Description:	Planned							CRW/G White					
AC-2(4)	Automated	Description:	Planned							CRW/G White					
AC-2(5)	Inactivity	Description:	Planned							CRW/G White					
AC-2(7)	Role-based	Description:	Planned							CRW/G White					
AC-2(9)	Restrictions On	Description:	Planned							CRW/G White					
AC-2(10)	Shared / Group	Description:	Planned							CRW/G Yellow					
AC-2(11)	Usage	Description:	Planned							CRW/G White					
AC-2(12)	Account	Description:	Planned							CRW/G White					
AC-2(13)	Disable	Description:	Planned							CRW/G Yellow					
AC-3	Access	Description:	Planned							CRW/G Yellow					
AC-3(4)	Discretionary	Description:	Planned							CRW/G White					
AC-4	Information	Description:	Planned							CRW/G Yellow					
AC-5	Separation Of	Description:	Planned							CRW/G White					
AC-6	Least Privilege	Description:	Planned							CRW/G White					
AC-6(1)	Authorize	Description:	Planned							CRW/G Yellow					
AC-6(2)	Non-privileged	Description:	Planned							CRW/G Yellow					
AC-6(3)	Network	Description:	Planned							CRW/G Yellow					
AC-6(5)	Privileged	Description:	Planned							CRW/G Yellow					
AC-6(7)	Review Of Use	Description:	Planned							CRW/G Yellow					
AC-6(8)	Privilege	Description:	Planned							CRW/G Yellow					
AC-6(9)	Auditing Use	Description:	Planned							CRW/G White					
AC-6(10)	Prohibit Non-	Description:	Planned							CRW/G White					
AC-7	Unsuccessful	Description:	Planned							CRW/G Yellow					
AC-8	System Use	Description:	Planned							CRW/G White					
AC-10	Concurrent	Description:	Planned							CRW/G White					
AC-11	Session Lock	Description:	Planned							CRW/G White					
AC-11(1)	Pattern-hiding	Description:	Planned							CRW/G White					
AC-12	Session	Description:	Planned							CRW/G Yellow					
AC-12(1)	User-initiated	Description:	Planned							CRW/G Yellow					
AC-14	Permitted	Description:	Planned							CRW/G White					



Step 3 – Implement Controls

Step 3
IMPLEMENT
Security Controls

CCIs for Baseline Controls based on CNSSI 1253
Several User options for tailoring population of form
Populated Test Results to template fields

Control / AP Information						Enter Test Results Here				Latest Test Results				
Control Number	Control Information	AP Acronym	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Compliance Status	Date Tested	Tested By	Test Results	Compliance Status	Date Tested	Tested By	Test Results
AC-1	Description: The organization: a. Develops, documents, and disseminates to (Assignment: organization-defined personnel or roles) 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	AC-13	000001	The organization develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among	The organization being inspected/assessed develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among	The organization conducting the inspection/assessment obtains and examines the access control policy to ensure the organization being inspected/assessed develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment.								
AC-1	Description: The organization: a. Develops, documents, and disseminates to (Assignment: organization-defined personnel or roles) 1. An access control policy that addresses purpose, scope, roles, responsibilities, management	AC-14	000002	The organization disseminates the access control policy to organization-defined personnel or roles.	The organization being inspected/assessed disseminates via an information sharing capability to all personnel. DoD has defined the personnel or roles as all	The organization conducting the inspection/assessment examines the access control policy via the organization's information sharing capability to ensure the organization being inspected/assessed disseminates								
AC-1	Description: The organization: a. Develops, documents, and disseminates to (Assignment: organization-defined personnel or roles) 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational	AC-15	000004	The organization develops and documents procedures to facilitate the implementation of the access control policy and associated access controls.	The organization being inspected/assessed develops and documents procedures to facilitate the implementation of the access control policy and associated access controls.	The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the access control policy and associated access controls to ensure the organization being inspected/assessed develops and								
AC-1	Description: The organization: a. Develops, documents, and disseminates to (Assignment: organization-defined personnel or roles) 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current:	AC-16	000005	The organization disseminates the procedures to facilitate access control policy and associated access controls to the organization-defined personnel or roles.	The organization being inspected/assessed disseminates via an information sharing capability to all personnel the procedures to facilitate access control policy and associated access controls. DoD has defined the personnel or roles as all personnel.	The organization conducting the inspection/assessment examines the procedures to facilitate access control policy and associated access controls via the organization's information sharing capability to ensure the organization being inspected/assessed disseminates the procedures to all personnel. DoD has defined the personnel or roles as all personnel.								
AC-1	Description: The organization: a. Develops, documents, and disseminates to (Assignment: organization-defined personnel or roles) 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current:	AC-17	000009	The organization develops and documents procedures to facilitate the implementation of the access control policy and associated access controls.	The organization being inspected/assessed develops and documents procedures to facilitate the implementation of the access control policy and associated access controls.	The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the access control policy and associated access controls to ensure the organization being inspected/assessed develops and								



CCI Test Result Export Form

User Selected Overlay

User Selected Tier 1 & 2 Controls

User Policy Templates

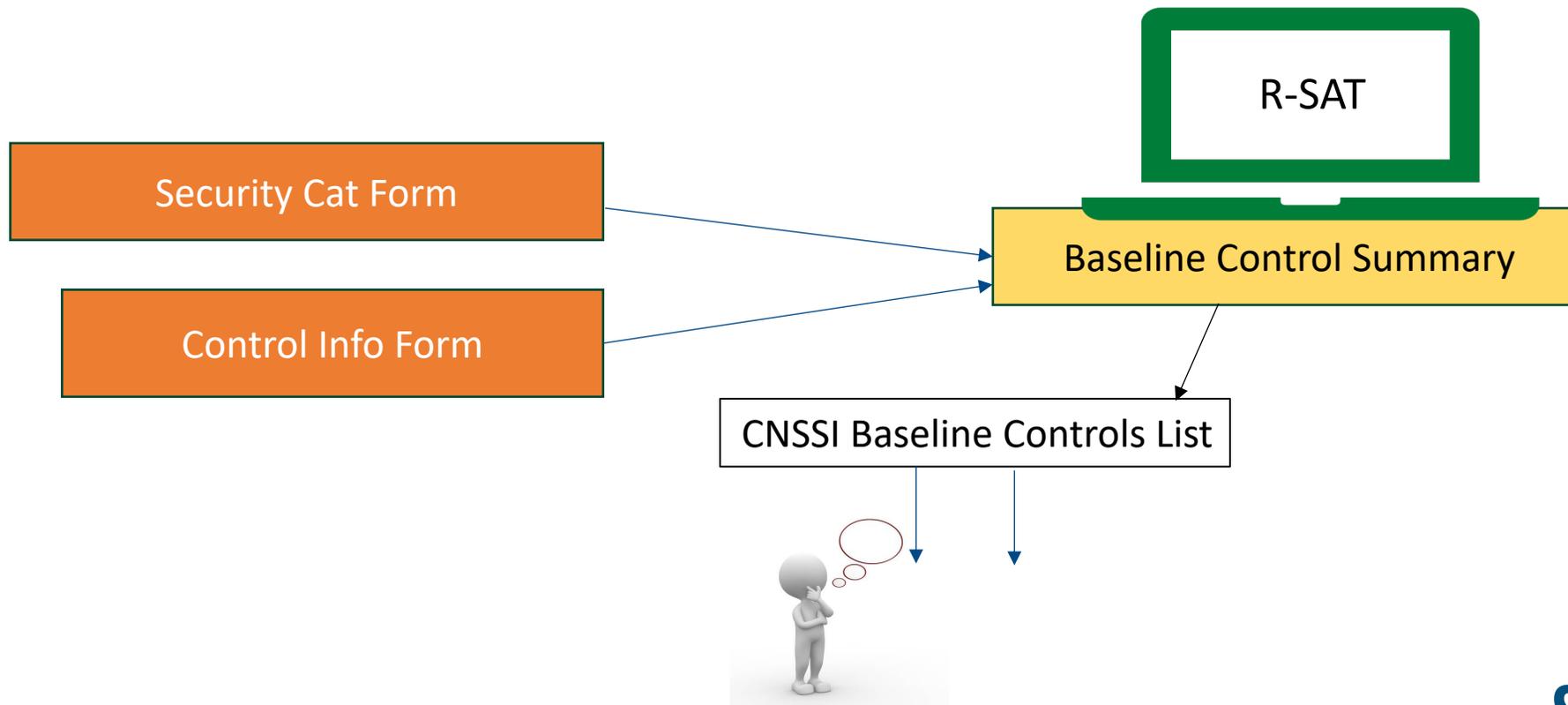
User Selected UFC 4-010-06

CNSSI Baseline Control CCIs

Test Results

Baseline Control Summary

Baseline Control Summary provides User with a list of controls applicable to the CIA Impact Levels and Overlay applied



Policy and Procedures Templates

Optional Templates

Risk Management Framework
Access Control (AC)
Policy and Procedures
[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

DISTRIBUTION STATEMENT C:
Distribution authorized to U.S. Government Agencies and their
Administrative or Operational Use. Other requests for this document
referred to the [ORGANIZATION NAME].

For Official Use Only (FOUO)

For Official Use Only (FOUO)
Access Control (AC) Policy & Procedures

2. Account Management (AC-2)
Account management for the [FACILITY NAME] includes policies and procedures for privileged users, acceptable use and account tracking. [User accounts established must initially be established on the [FACILITY NAME] Sensitive But Unclassified Network]. The policy and procedures referenced in this document are specific to [FACILITY NAME] accounts.
System configurations for [FACILITY NAME] access control will follow Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs) and Security Readiness Guides (SRGs) to the extent possible. Exceptions will be noted in the checklists and distributed to the ISSO/ISSM, as well as the Authorizing Official or designee.
The ISSO will serve as the designated Account Manager and will approve the creation, modification, or removal of information system accounts CC-002112, CC-000010, CC-000011. The ISSM will notify the Account Manager if an account is no longer required, if a user is terminated or transferred, or if system usage or need-to-know changes CC-002121, CC-002123, CC-002124 and CC-002125. The ISSO will be the account managers for the [FACILITY NAME] control system and will ensure that all system users require access to the system for approved job functions CC-002113, CC-002115. The assigned system accounts shall be reviewed by the ISSM at least annually for compliance with "need-to-know" requirements. CC-000012. Account usage is monitored by the ISSM on a monthly basis by reviewing [audit logs] CC-002122.
The ISSO or designee will maintain a list of authorized users on the Master Authorized User List (Master AUL) [local file: LogShare\au\Master AUL] CC-000008. Only authorized representatives of the [FACILITY NAME] and company representatives with active contracts with these organizations, who have a mission, administrative, or security function on the [FACILITY NAME] control system, will be authorized to access the system. To obtain an account and appropriate credentials, users will be required to complete all cybersecurity awareness training, along with any required training specific to the assigned job function. The Account Manager will verify training records and user's organization and functional roles prior to approving and authorizing access. Group accounts are not allowed CC-002116, CC-002129.

3. Access Enforcement (AC-3)
The DoD Standard Notice of Consent and Acceptable Use Policy (AUP) for authorized users are included in Appendix A and B. The [FACILITY NAME] will require authorized users to read and sign the DoD Standard Notice of Consent and AUP and the data is recorded on the Master AUL. CC-000213. The AUP and PAUP are also referenced in the [FACILITY NAME] Personnel Security Policy and Procedures document.

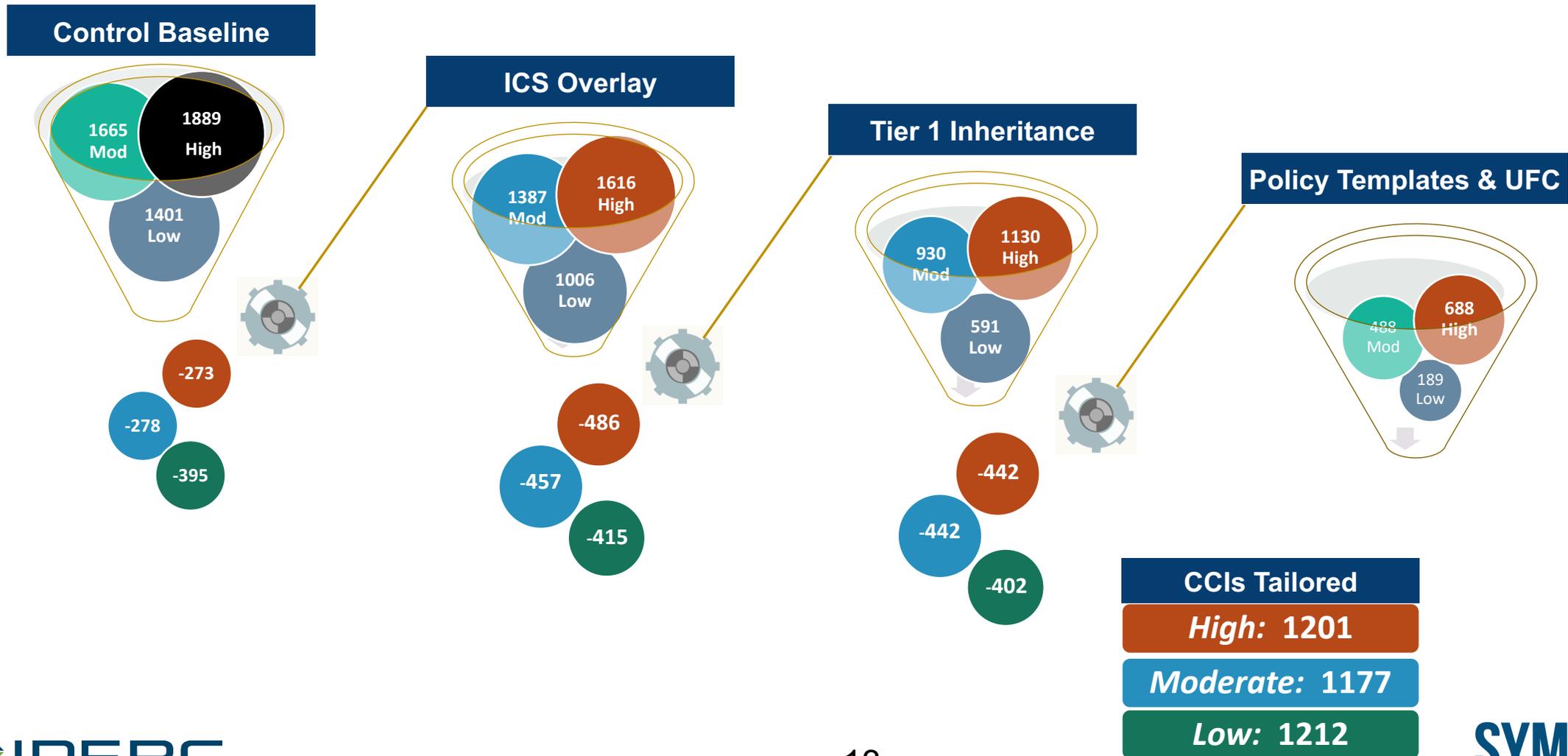
AC-5 Separation of Duties for Moderate Level systems:
The ISSO implements processes to maintain separation of job duties for individuals that use the system to ensure that all system users require limited access for approved job functions CC-000016, CC-001180, CC-002219, CC-002220.

AC-6(1) Least Privilege – Authorized Access for Moderate Level systems:
The ISSO and the ICS allow access to authorize access to functions and information that is not publicly available. Authorized users will be tracked on the Master Authorized User List (Excel file:

Update Form	Export	Remote Facility	Confidentiality: Low	Integrity: Moderate	Availability: Moderate
-------------	--------	-----------------	-------------------------	------------------------	---------------------------

		on		Test Results							
Control	Control	Assessment	Compliance	Date Tested	Tested By	Test Results					
AC-1	Description: The organization	AC-1.3 000001	The organization develops and documents	The organization being inspected/assessed	The organization conducting the inspection/assessment obtains and examines the access	Compliant	04-Dec-2019	Doug Demo	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document.		

CCI Baseline Impacts





Facility-Related Control System RMF Self-Assessment Tool R-SAT

Aura Lee Keating

IPERC

Auralee.Keating@ipercc.com

Denise Hanus

IPERC

Denise.Hanus@ipercc.com



SERDP • ESTCP
SYMPOSIUM
2019 | Enhancing DoD's Mission Effectiveness