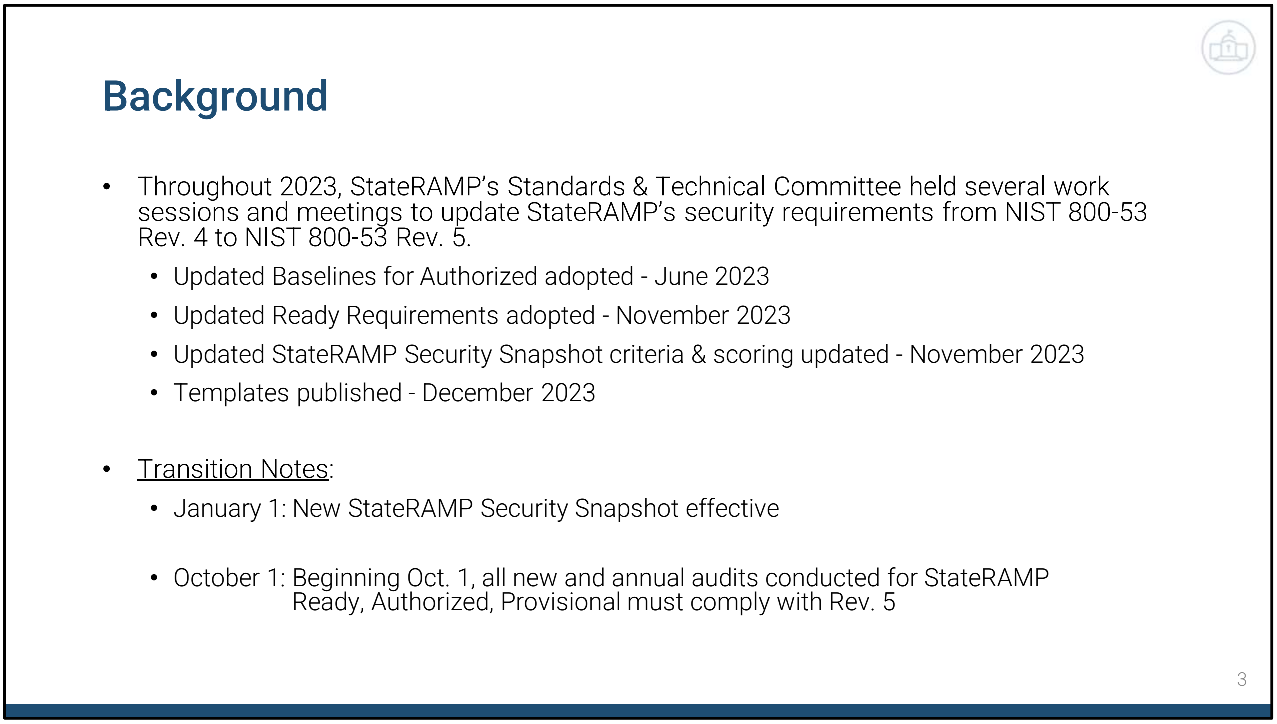
StateRAMP

Office Hours

Special Edition: Rev. 5
January 17, 2024



Background

- Throughout 2023, StateRAMP's Standards & Technical Committee held several work sessions and meetings to update StateRAMP's security requirements from NIST 800-53 Rev. 4 to NIST 800-53 Rev. 5.
  - Updated Baselines for Authorized adopted - June 2023
  - Updated Ready Requirements adopted - November 2023
  - Updated StateRAMP Security Snapshot criteria & scoring updated - November 2023
  - Templates published - December 2023

- Transition Notes:
  - January 1: New StateRAMP Security Snapshot effective
  - October 1: Beginning Oct. 1, all new and annual audits conducted for StateRAMP Ready, Authorized, Provisional must comply with Rev. 5

Last year, the StateRAMP Standards & Technical Committee reviewed and updated all StateRAMP security requirements and policies to transition from NIST 800-53 Rev. 4 to the most recent publication, NIST 800-53 Rev. 5 that has updated control families and improved guidance for cloud security best practices.

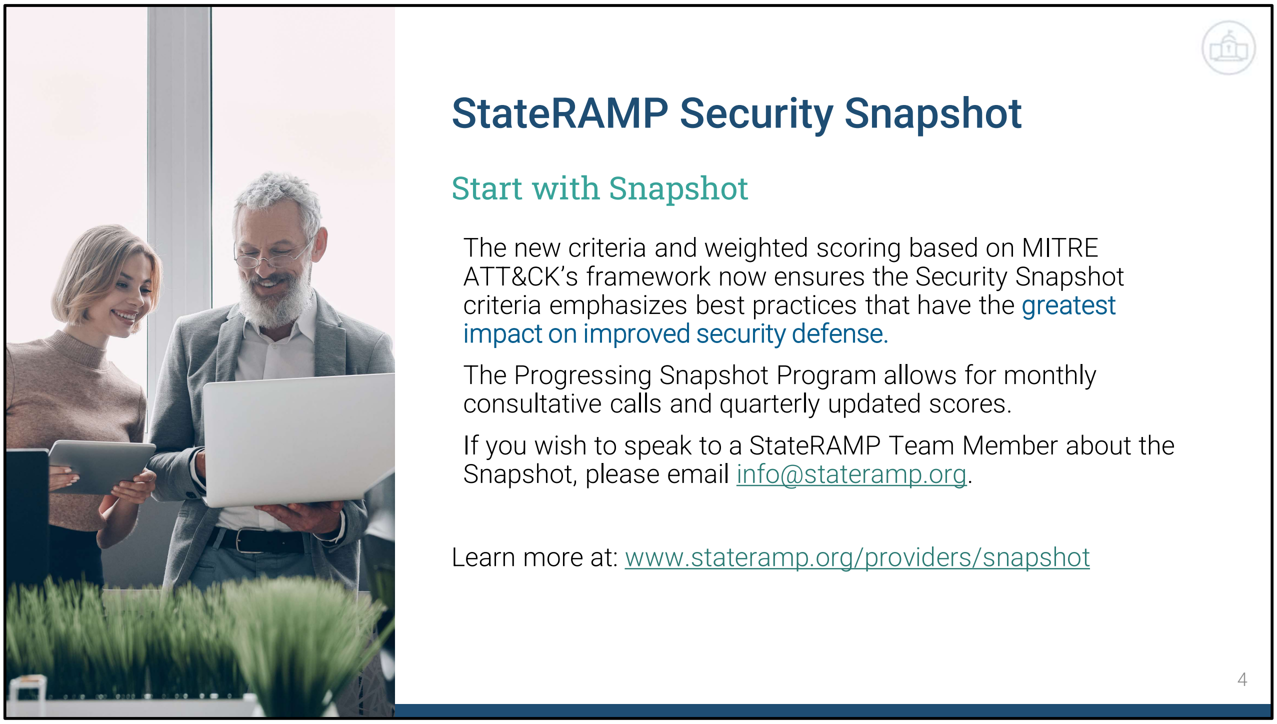
The updated Security Snapshot is in effect, as of January 1, 2024

All new security packages for Ready/Authorized submitted on October 1 onward will need to comply with the new Rev. 5 requirements.

All annual audits submitted for Ready/Authorized submitted on October 1 onward will need to comply with the new Rev. 5 requirements.

Those wishing to move to Rev. 5 can do so before October 1. October 1 will be the date when Rev. 5 will be required for new packages / audits submitted for review.

Until October 1, the PMO will be accepting packages based on Rev. 4 requirements during this transition period.



StateRAMP Security Snapshot

Start with Snapshot

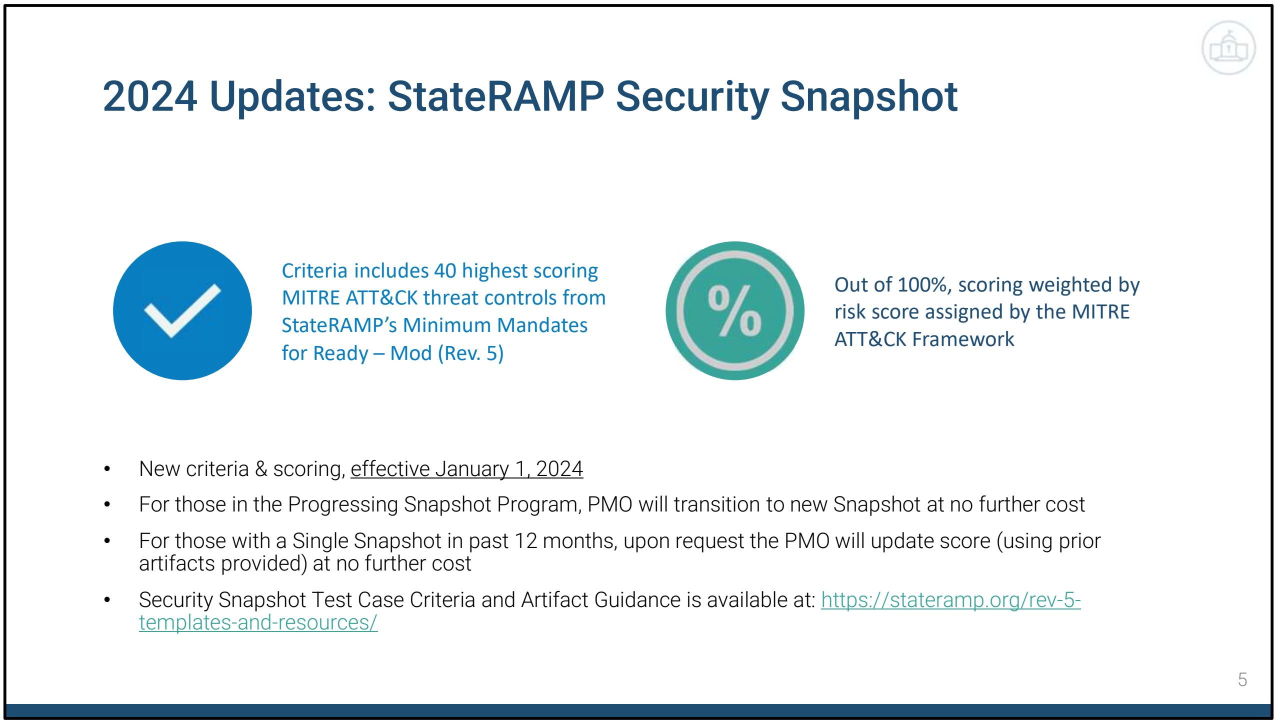
The new criteria and weighted scoring based on MITRE ATT&CK's framework now ensures the Security Snapshot criteria emphasizes best practices that have the greatest impact on improved security defense.

The Progressing Snapshot Program allows for monthly consultative calls and quarterly updated scores.

If you wish to speak to a StateRAMP Team Member about the Snapshot, please email info@stateramp.org.

Learn more at: www.stateramp.org/providers/snapshot

StateRAMP's security program starts with the Snapshot. The Snapshot Criteria and Scoring has been updated, and we are very excited about the novel approach which ties in the MITRE Attack Framework and now ensure the snapshot criteria emphasizes the best practices that have the greatest impact on improved security defenses.



2024 Updates: StateRAMP Security Snapshot

✓ Criteria includes 40 highest scoring MITRE ATT&CK threat controls from StateRAMP's Minimum Mandates for Ready – Mod (Rev. 5)

% Out of 100%, scoring weighted by risk score assigned by the MITRE ATT&CK Framework

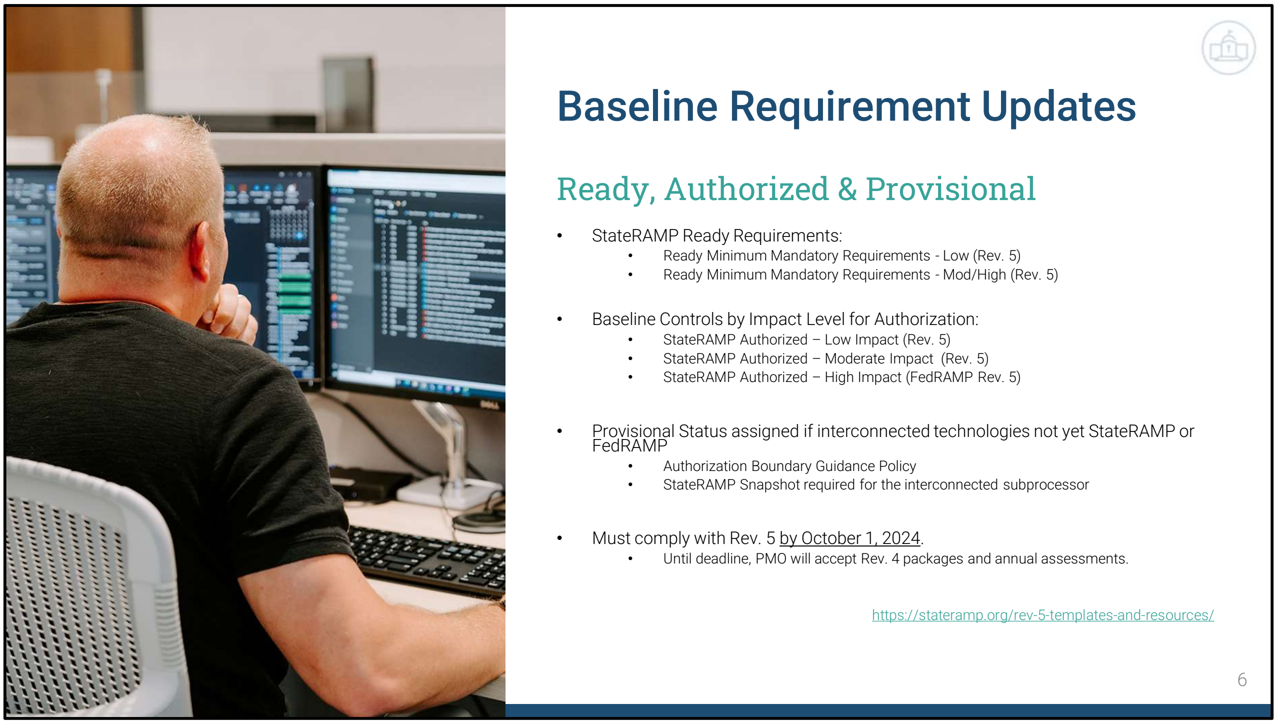
- New criteria & scoring, effective January 1, 2024
- For those in the Progressing Snapshot Program, PMO will transition to new Snapshot at no further cost
- For those with a Single Snapshot in past 12 months, upon request the PMO will update score (using prior artifacts provided) at no further cost
- Security Snapshot Test Case Criteria and Artifact Guidance is available at: https://stateramp.org/rev-5-templates-and-resources/

The StateRAMP Security Snapshot criteria and scoring has had two important updates that are in effect as of Jan. 1.

1) The criteria is updated to include the 40 highest scoring MITRE ATT&CK threat controls from the requirements for StateRAMP Ready – Mod Impact.
2) The scoring has changed from 60 points to a percentage out of 100, weighted by risk score assigned by the MITRE Attack Framework. The higher the weighting, the higher the threat score importance.

New criteria & scoring, effective January 1, 2024
For those in Progressing Snapshot Program, PMO will transition to new Snapshot at no further cost
For those with a Single Snapshot in past 12 months, PMO will update score (using prior artifacts provided) at no further cost

View the new Snapshot Criteria and Scoring available at: https://stateramp.org/rev-5-templates-and-resources/



Baseline Requirement Updates

Ready, Authorized & Provisional

- StateRAMP Ready Requirements:
  - Ready Minimum Mandatory Requirements - Low (Rev. 5)
  - Ready Minimum Mandatory Requirements - Mod/High (Rev. 5)
- Baseline Controls by Impact Level for Authorization:
  - StateRAMP Authorized – Low Impact (Rev. 5)
  - StateRAMP Authorized – Moderate Impact (Rev. 5)
  - StateRAMP Authorized – High Impact (FedRAMP Rev. 5)
- Provisional Status assigned if interconnected technologies not yet StateRAMP or FedRAMP
  - Authorization Boundary Guidance Policy
  - StateRAMP Snapshot required for the interconnected subprocessor
- Must comply with Rev. 5 by October 1, 2024.
  - Until deadline, PMO will accept Rev. 4 packages and annual assessments.

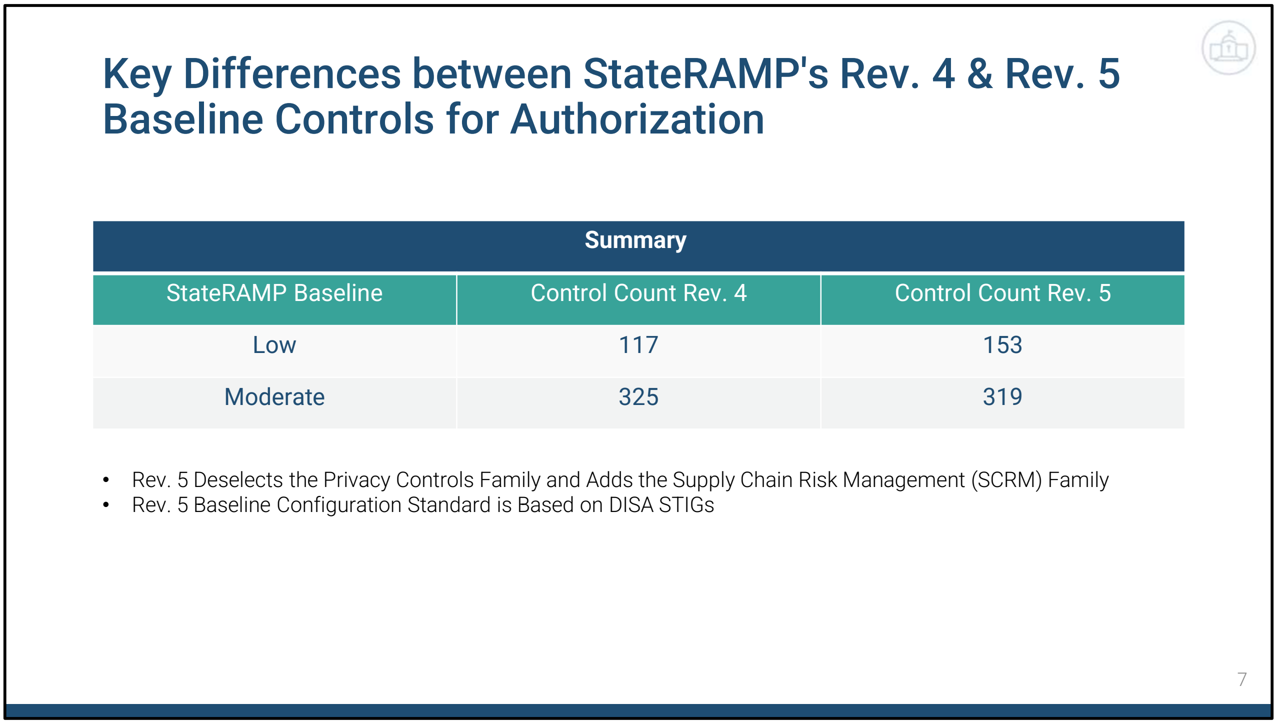
https://stateramp.org/rev-5-templates-and-resources/

The baseline security control requirements were updated for all of StateRAMP’s Security Statuses: Ready and Authorized.

The following documents were updated, including:
- Ready Requirements for both Low and Moderate/High Impact Levels
- Baseline Controls for Authorization for Low and Moderate Impact levels. (Note: we recognize FedRAMP’s High Impact Level)

Provisional is a status that was updated in 2023 as well.
A Provisional Status may be assigned if a package is submitted for Authorization, but interconnected technologies are not StateRAMP or FedRAMP Authorized.
As Supply Chain risks grow, ensuring interconnected technologies meet minimum requirements is important.

All of these baseline controls can be found on the website.

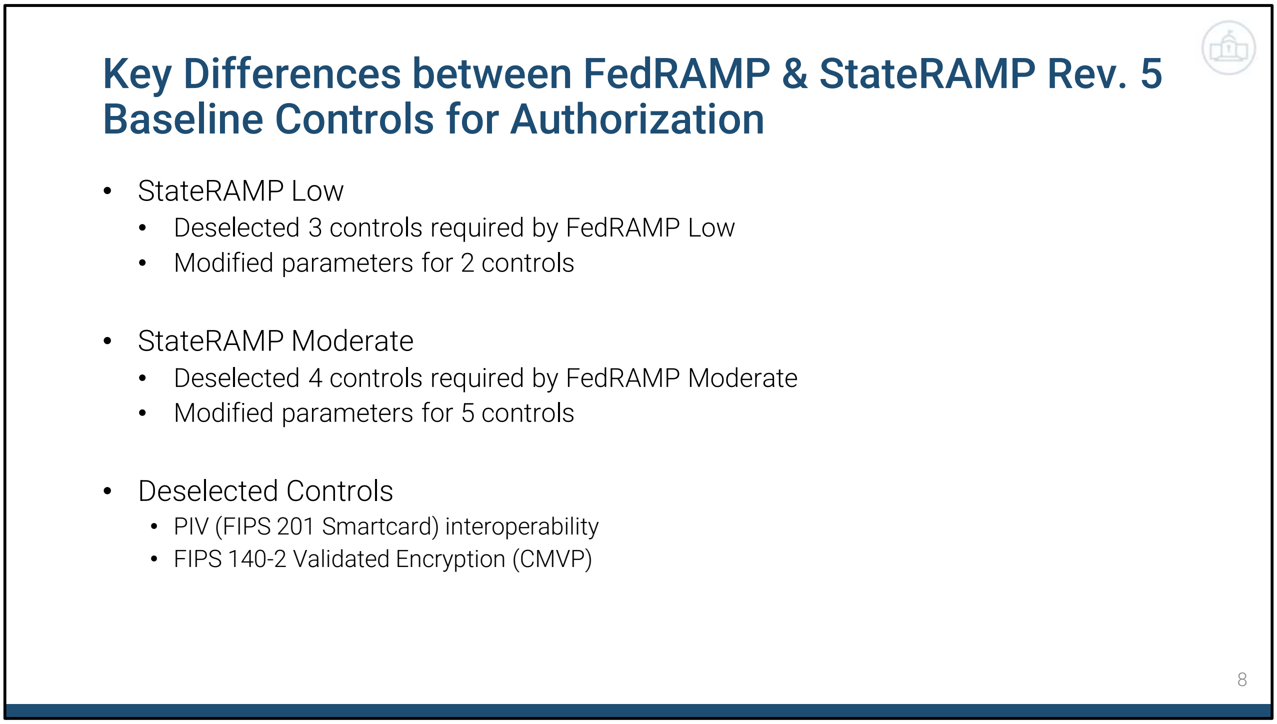


Key Differences between StateRAMP's Rev. 4 & Rev. 5 Baseline Controls for Authorization

Summary		
StateRAMP Baseline	Control Count Rev. 4	Control Count Rev. 5
Low	117	153
Moderate	325	319

- Rev. 5 Deselects the Privacy Controls Family and Adds the Supply Chain Risk Management (SCRM) Family
- Rev. 5 Baseline Configuration Standard is Based on DISA STIGs

Here you can see the differences highlighted from Rev. 4 requirements to Rev. 5.



Key Differences between FedRAMP & StateRAMP Rev. 5 Baseline Controls for Authorization

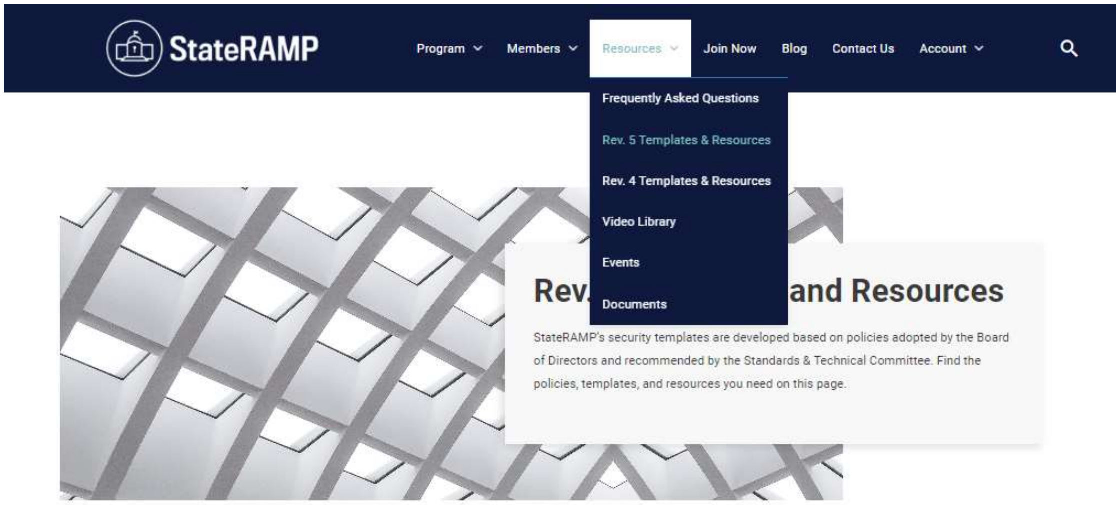
- StateRAMP Low
  - Deselected 3 controls required by FedRAMP Low
  - Modified parameters for 2 controls
- StateRAMP Moderate
  - Deselected 4 controls required by FedRAMP Moderate
  - Modified parameters for 5 controls
- Deselected Controls
  - PIV (FIPS 201 Smartcard) interoperability
  - FIPS 140-2 Validated Encryption (CMVP)

Although StateRAMP does not require PIV cards, we still require phishing resistant multi-factor authentication.

StateRAMP does not require cryptographic modules to be validated under the NIST Cryptographic Module Validation Program (CMVP), however we do require the algorithms to be modern.

Resources

https://stateramp.org/rev-5-templates-and-resources/



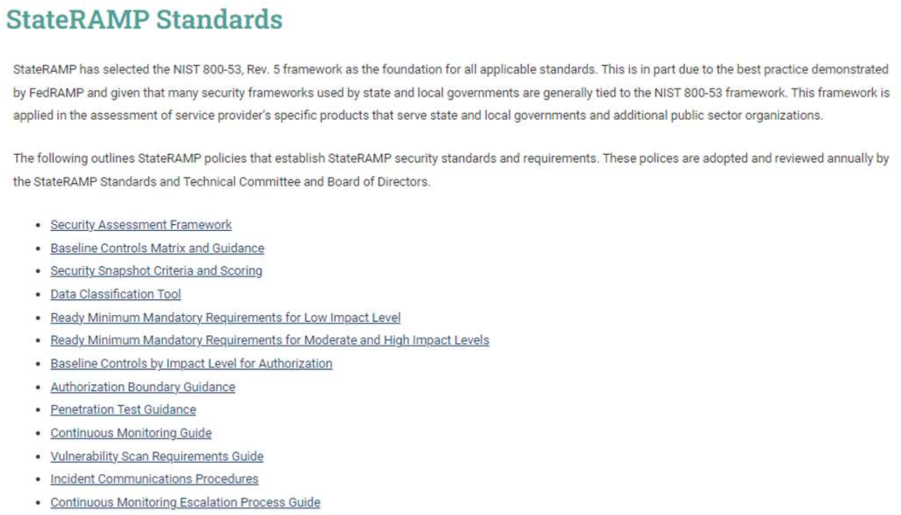
Rev. … and Resources

StateRAMP's security templates are developed based on policies adopted by the Board of Directors and recommended by the Standards & Technical Committee. Find the policies, templates, and resources you need on this page.

The policies and templates are published on the StateRAMP Website.
When you click on Resources tab, you will see two options – one for Rev. 5 and one for Rev. 4

Resources

https://stateramp.org/rev-5-templates-and-resources/



StateRAMP Standards

StateRAMP has selected the NIST 800-53, Rev. 5 framework as the foundation for all applicable standards. This is in part due to the best practice demonstrated by FedRAMP and given that many security frameworks used by state and local governments are generally tied to the NIST 800-53 framework. This framework is applied in the assessment of service provider's specific products that serve state and local governments and additional public sector organizations.

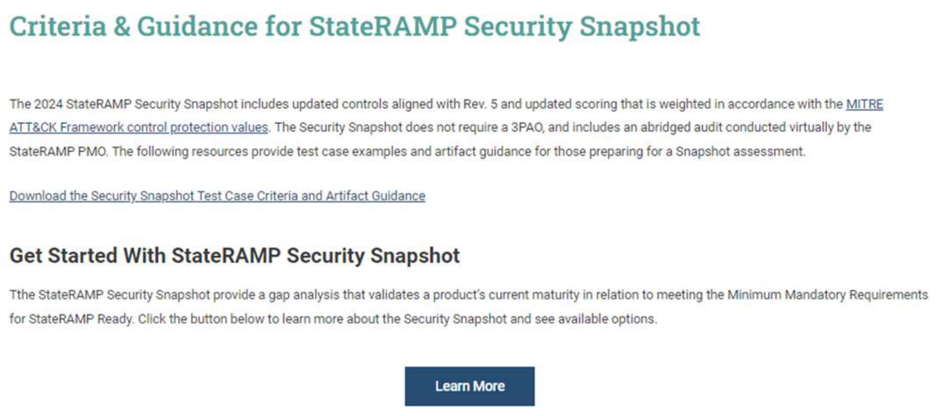
The following outlines StateRAMP policies that establish StateRAMP security standards and requirements. These polices are adopted and reviewed annually by the StateRAMP Standards and Technical Committee and Board of Directors.

- Security Assessment Framework
- Baseline Controls Matrix and Guidance
- Security Snapshot Criteria and Scoring
- Data Classification Tool
- Ready Minimum Mandatory Requirements for Low Impact Level
- Ready Minimum Mandatory Requirements for Moderate and High Impact Levels
- Baseline Controls by Impact Level for Authorization
- Authorization Boundary Guidance
- Penetration Test Guidance
- Continuous Monitoring Guide
- Vulnerability Scan Requirements Guide
- Incident Communications Procedures
- Continuous Monitoring Escalation Process Guide

On Rev. 5 Page, you will see the StateRAMP Standards and links to each policy that are approved by the StateRAMP Standards & Technical Committee and adopted by the StateRAMP Board of Directors.

Resources

https://stateramp.org/rev-5-templates-and-resources/



Criteria & Guidance for StateRAMP Security Snapshot

The 2024 StateRAMP Security Snapshot includes updated controls aligned with Rev. 5 and updated scoring that is weighted in accordance with the MITRE ATT&CK Framework control protection values. The Security Snapshot does not require a 3PAO, and includes an abridged audit conducted virtually by the StateRAMP PMO. The following resources provide test case examples and artifact guidance for those preparing for a Snapshot assessment.

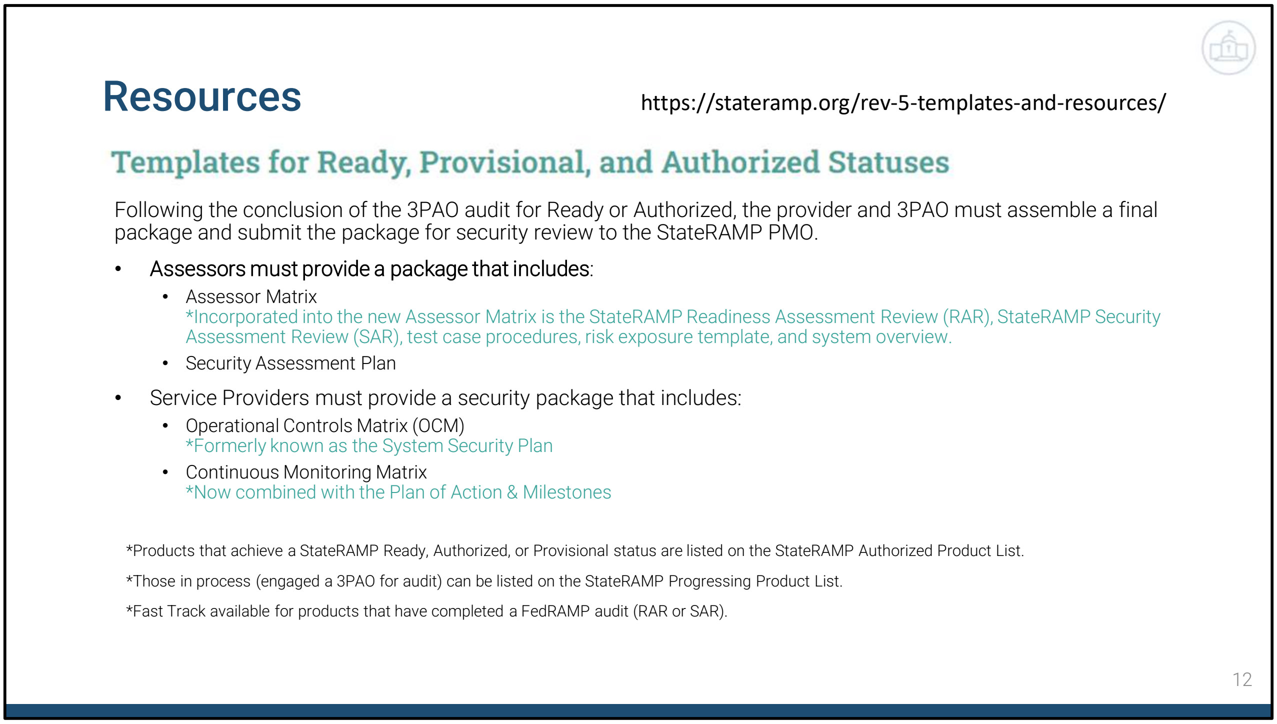
Download the Security Snapshot Test Case Criteria and Artifact Guidance

Get Started With StateRAMP Security Snapshot

Tthe StateRAMP Security Snapshot provide a gap analysis that validates a product's current maturity in relation to meeting the Minimum Mandatory Requirements for StateRAMP Ready. Click the button below to learn more about the Security Snapshot and see available options.

Note: Products enrolled in the Progressing Snapshot Program are listed on the Progressing Product List.

As you scroll down the page, you will see information about the StateRAMP Security Snapshot



Resources

https://stateramp.org/rev-5-templates-and-resources/

Templates for Ready, Provisional, and Authorized Statuses

Following the conclusion of the 3PAO audit for Ready or Authorized, the provider and 3PAO must assemble a final package and submit the package for security review to the StateRAMP PMO.

- Assessors must provide a package that includes:
  - Assessor Matrix
    *Incorporated into the new Assessor Matrix is the StateRAMP Readiness Assessment Review (RAR), StateRAMP Security Assessment Review (SAR), test case procedures, risk exposure template, and system overview.
  - Security Assessment Plan
- Service Providers must provide a security package that includes:
  - Operational Controls Matrix (OCM)
    *Formerly known as the System Security Plan
  - Continuous Monitoring Matrix
    *Now combined with the Plan of Action & Milestones

*Products that achieve a StateRAMP Ready, Authorized, or Provisional status are listed on the StateRAMP Authorized Product List.

*Those in process (engaged a 3PAO for audit) can be listed on the StateRAMP Progressing Product List.

*Fast Track available for products that have completed a FedRAMP audit (RAR or SAR).

And, a description of what should be submitted for those seeking a StateRAMP Ready or Authorized Status.

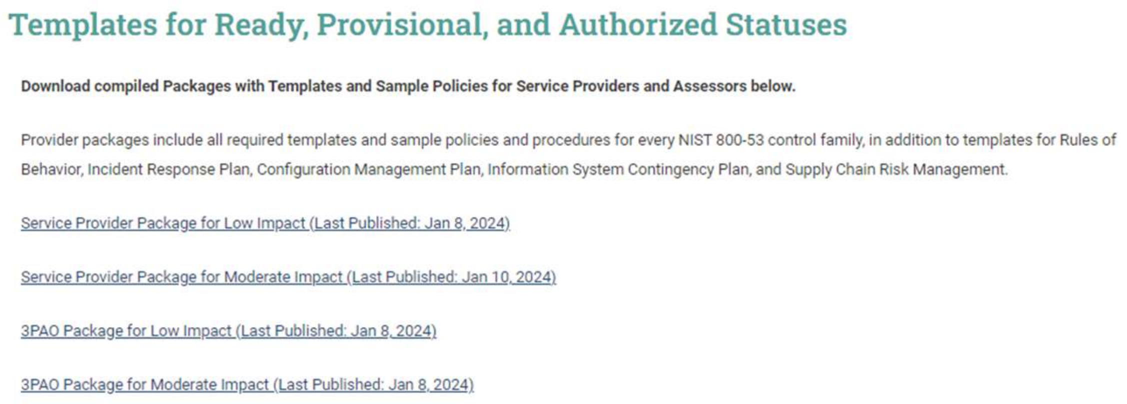
There are a few changes to note in these templates:
1) For the Assessors:
- *Assessor Matrix - Incorporated into the new Assessor Matrix is the StateRAMP Readiness Assessment Review (RAR), StateRAMP Security Assessment Review (SAR), test case procedures, risk exposure template, and system overview.

2) For the Service Providers:
- *Operational Controls Matrix -- Formerly known as the System Security Plan
- *Continuous Monitoring Matrix -- Now combined with a Plan of Action & Milestones

The Fast Track process is still in place for products that have completed a FedRAMP audit (RAR or SAR). Please note – they do not need to wait until receiving a FedRAMP Status to submit for the Fast Track. If they have completed a RAR or SAR, they can start with StateRAMP.

Resources

https://stateramp.org/rev-5-templates-and-resources/



Templates for Ready, Provisional, and Authorized Statuses

Download compiled Packages with Templates and Sample Policies for Service Providers and Assessors below.

Provider packages include all required templates and sample policies and procedures for every NIST 800-53 control family, in addition to templates for Rules of Behavior, Incident Response Plan, Configuration Management Plan, Information System Contingency Plan, and Supply Chain Risk Management.

Service Provider Package for Low Impact (Last Published: Jan 8, 2024)

Service Provider Package for Moderate Impact (Last Published: Jan 10, 2024)

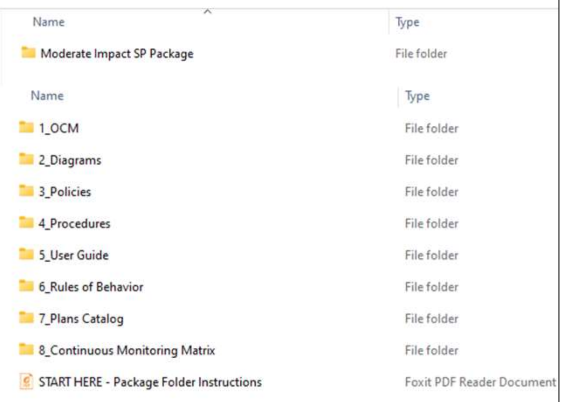
3PAO Package for Low Impact (Last Published: Jan 8, 2024)

3PAO Package for Moderate Impact (Last Published: Jan 8, 2024)

Further down on the Resources page, you will find the Templates packages. In the past, each individual document was a separate download link – for Rev. 5, we have published these templates as zipped folders for ease of download.

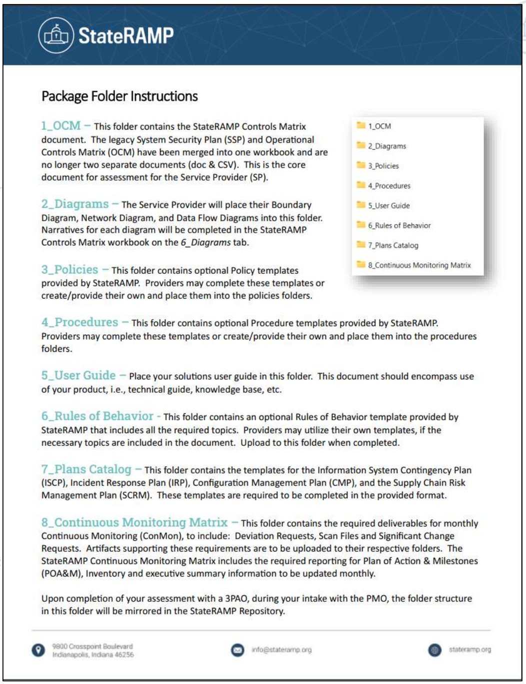
Resources

Package Folder Example



Name	Type
Moderate Impact SP Package	File folder

Name	Type
1_OCM	File folder
2_Diagrams	File folder
3_Policies	File folder
4_Procedures	File folder
5_User Guide	File folder
6_Rules of Behavior	File folder
7_Plans Catalog	File folder
8_Continuous Monitoring Matrix	File folder
START HERE - Package Folder Instructions	Foxit PDF Reader Document



StateRAMP

Package Folder Instructions

- 1_OCM
- 2_Diagrams
- 3_Policies
- 4_Procedures
- 5_User Guide
- 6_Rules of Behavior
- 7_Plans Catalog
- 8_Continuous Monitoring Matrix

1_OCM – This folder contains the StateRAMP Controls Matrix document. The legacy System Security Plan (SSP) and Operational Controls Matrix (OCM) have been merged into one workbook and are no longer two separate documents (doc & CSV). This is the core document for assessment for the Service Provider (SP).

2_Diagrams – The Service Provider will place their Boundary Diagram, Network Diagram, and Data Flow Diagrams into this folder. Narratives for each diagram will be completed in the StateRAMP Controls Matrix workbook on the *6_Diagrams* tab.

3_Policies – This folder contains optional Policy templates provided by StateRAMP. Providers may complete these templates or create/provide their own and place them into the policies folders.

4_Procedures – This folder contains optional Procedure templates provided by StateRAMP. Providers may complete these templates or create/provide their own and place them into the procedures folders.

5_User Guide – Place your solutions user guide in this folder. This document should encompass use of your product, i.e., technical guide, knowledge base, etc.

6_Rules of Behavior - This folder contains an optional Rules of Behavior template provided by StateRAMP that includes all the required topics. Providers may utilize their own templates, if the necessary topics are included in the document. Upload to this folder when completed.

7_Plans Catalog – This folder contains the templates for the Information System Contingency Plan (ISCP), Incident Response Plan (IRP), Configuration Management Plan (CMP), and the Supply Chain Risk Management Plan (SCRM). These templates are required to be completed in the provided format.

8_Continuous Monitoring Matrix – This folder contains the required deliverables for monthly Continuous Monitoring (ConMon), to include: Deviation Requests, Scan Files and Significant Change Requests. Artifacts supporting these requirements are to be uploaded to their respective folders. The StateRAMP Continuous Monitoring Matrix includes the required reporting for Plan of Action & Milestones (POA&M), Inventory and executive summary information to be updated monthly.

Upon completion of your assessment with a 3PAO, during your intake with the PMO, the folder structure in this folder will be mirrored in the StateRAMP Repository.

9800 Crosspoint Boulevard
Indianapolis, Indiana 46256

info@stateramp.org

stateramp.org

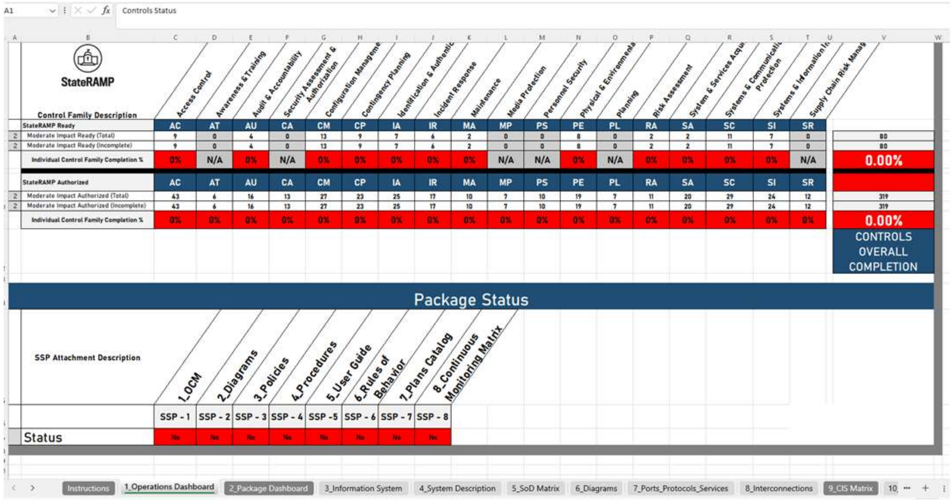
When you download a folder, we recommend opening the document titled START HERE first as it will describe the package folder contents for you.

If you have questions, as always reach out to info@stateramp.org or attend our regularly scheduled Office Hours. Visit https://stateramp.org/events for the schedule

Resources

https://stateramp.org/rev-5-templates-and-resources/

Controls Matrix Example



A1 | Controls Status

StateRAMP

Control Family Description	Access Control	Awareness & Training	Audit & Accountability	Security Assessment & Authorization	Configuration Manageme	Contingency Planning	Identification & Authentic	Incident Response	Maintenance	Media Protection	Personnel Security	Physical & Environmenta	Planning	Risk Assessment	System & Services Acqu	Systems & Communicatio Protection	Systems & Information In	Supply Chain Risk Manag	
StateRAMP Ready	AC	AT	AU	CA	CM	CP	IA	IR	MA	MP	PS	PE	PL	RA	SA	SC	SI	SR	
Moderate Impact Ready (Total)	9	0	4	0	13	9	7	6	2	0	0	8	0	2	2	11	7	0	80
Moderate Impact Ready (Incomplete)	9	0	4	0	13	9	7	6	2	0	0	8	0	2	2	11	7	0	80
Individual Control Family Completion %	0%	N/A	0%	N/A	0%	0%	0%	0%	0%	N/A	N/A	0%	N/A	0%	0%	0%	0%	N/A	0.00%
StateRAMP Authorized	AC	AT	AU	CA	CM	CP	IA	IR	MA	MP	PS	PE	PL	RA	SA	SC	SI	SR	
Moderate Impact Authorized (Total)	43	6	16	13	27	23	25	17	10	7	10	19	7	11	20	29	24	12	319
Moderate Impact Authorized (Incomplete)	43	6	16	13	27	23	25	17	10	7	10	19	7	11	20	29	24	12	319
Individual Control Family Completion %	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0.00%

CONTROLS OVERALL COMPLETION

Package Status

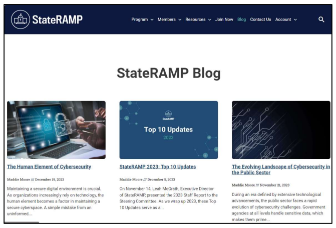
SSP Attachment Description	1_OCM	2_Diagrams	3_Policies	4_Procedures	5_User Guide	6_Rules of Behavior	7_Plans Catalog	8_Continuous Monitoring Matrix
	SSP - 1	SSP - 2	SSP - 3	SSP - 4	SSP -5	SSP - 6	SSP - 7	SSP - 8
Status	No	No	No	No	No	No	No	No

The last document to bring to your attention is the updated Controls Matrix. The dashboard tab currently shown is built to allow for ease of tracking of progress with information all contained in one (easier to use) workbook. As you complete items, those reds turn to green.

StateRAMP Office Hours

Other resources

- StateRAMP Blog
  - https://stateramp.org/blog/
- Monthly StateRAMP Member Newsletter
  - https://stateramp.org/newsletter-signup/



StateRAMP Blog

The Human Element of Cybersecurity

Maddie Moore /// December 19, 2023

Maintaining a secure digital environment is crucial. As organizations increasingly rely on technology, the human element becomes a factor in maintaining a secure cyberspace. A simple mistake from an uninformed...

StateRAMP 2023: Top 10 Updates

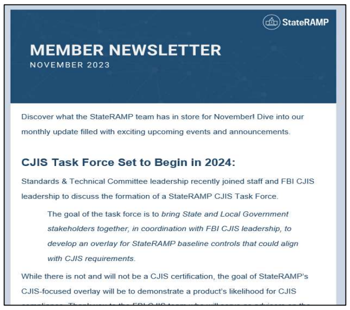
Maddie Moore /// December 5, 2023

On November 14, Leah McGrath, Executive Director of StateRAMP, presented the 2023 Staff Report to the Steering Committee. As we wrap up 2023, these Top 10 Updates serve as a...

The Evolving Landscape of Cybersecurity in the Public Sector

Maddie Moore /// November 21, 2023

During an era defined by extensive technological advancements, the public sector faces a rapid evolution of cybersecurity challenges. Government agencies at all levels handle sensitive data, which makes them prime...



MEMBER NEWSLETTER
NOVEMBER 2023

Discover what the StateRAMP team has in store for November! Dive into our monthly update filled with exciting upcoming events and announcements.

CJIS Task Force Set to Begin in 2024:

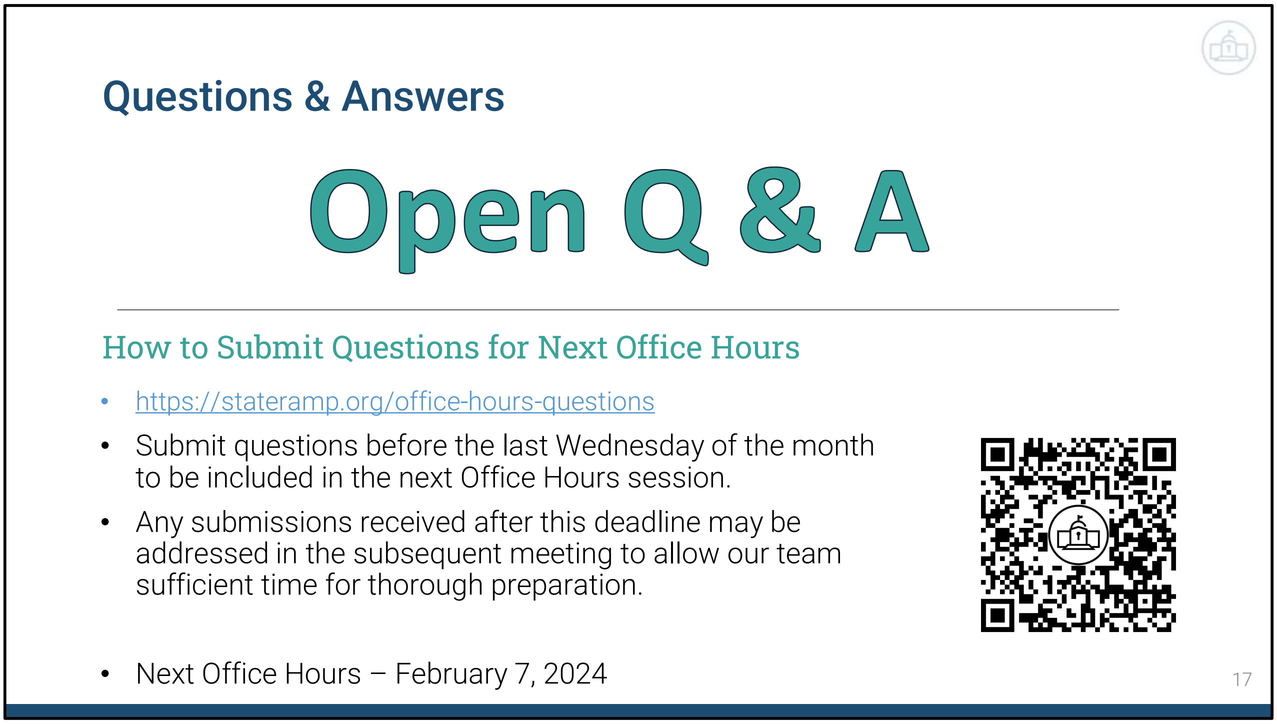
Standards & Technical Committee leadership recently joined staff and FBI CJIS leadership to discuss the formation of a StateRAMP CJIS Task Force.

> The goal of the task force is to *bring State and Local Government stakeholders together, in coordination with FBI CJIS leadership, to develop an overlay for StateRAMP baseline controls that could align with CJIS requirements.*

While there is not and will not be a CJIS certification, the goal of StateRAMP's CJIS-focused overlay will be to demonstrate a product's likelihood for CJIS

**StateRAMP
Newsletter Sign Up**

Two additional resources available to help you keep up to date on all things StateRAMP are the StateRAMP Blog and the StateRAMP Member Newsletter presented monthly by the Leah McGrath, the Executive Director of StateRAMP.   You can sign up now using the QR code on your screen.



Questions & Answers

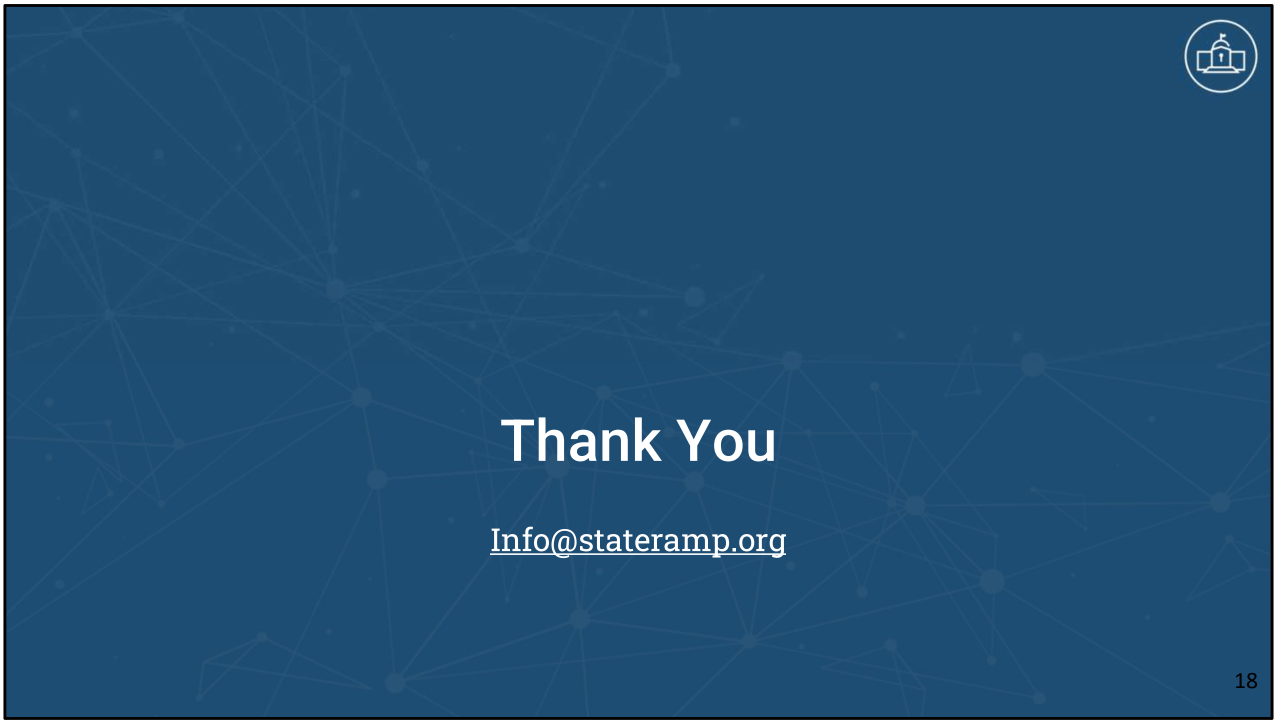
Open Q & A

How to Submit Questions for Next Office Hours

- https://stateramp.org/office-hours-questions
- Submit questions before the last Wednesday of the month to be included in the next Office Hours session.
- Any submissions received after this deadline may be addressed in the subsequent meeting to allow our team sufficient time for thorough preparation.

- Next Office Hours – February 7, 2024

17



Thank You

Info@stateramp.org

18

As we put these templates and documents to work, we do anticipate updates. For the most part, if you've already begun your work – don't worry about updating to new forms. We will let you know in office hours, emails and on the website if there are any updates to any forms that are required for you to use.

With our remaining time, we are happy to answer any questions you have.