Understanding GovRAMP From An Agency Procurement Overview

Michael McCray / Andrea Pacyna

PEAK

SMARTER PROCUREMENT
FOR PUBLIC GOOD

Agenda

- What is GovRAMP?
- How does it effect state purchasing and procurement?
- GovRAMP Security Framework and Statuses
- North Carolina’s GovRAMP Implementation
- Q&A

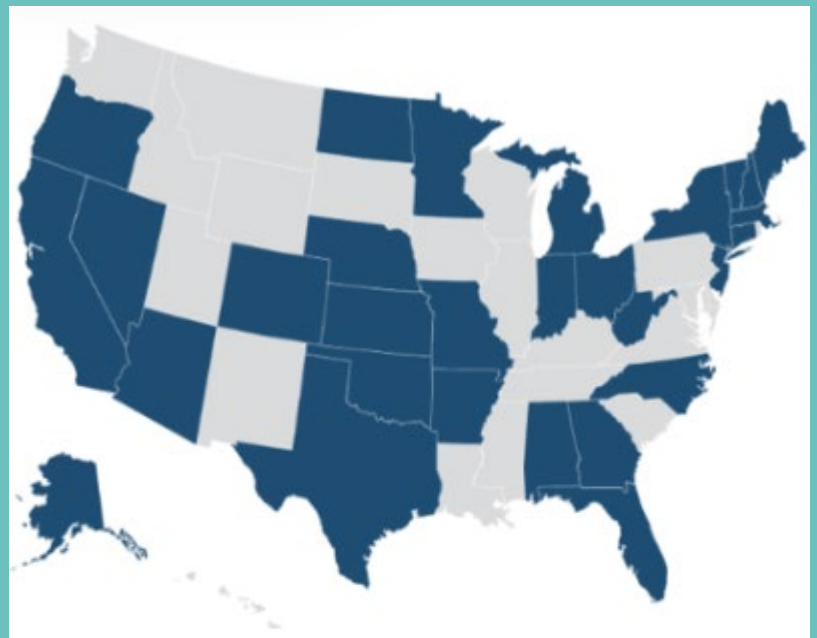
What is GovRAMP?

CREATING A FRAMEWORK FOR CONTINUOUS IMPROVEMENT IN CYBERSECURITY FOR N.C., ITS PROVIDERS, AND THE CONSTITUENTS THEY SERVE. IT APPLIES TO VENDOR HOSTED SOLUTIONS ONLY.

GovRAMP – Verify Once, Serve Many

As a result of partnership with GovRAMP:

- ✓ **Service providers complete one comprehensive verification process,** including continuous monitoring, that is shared with GovRAMP's participating organizations.
- ✓ **Governments can increase efficiency in procuring verified cloud products** and reduce costs of managing cybersecurity risk.
- ✓ **Governments and service providers are united under one standardized framework** to validate the cybersecurity posture of cloud products serving the public sector.



GovRAMP partners with:

- 29 states
- 14 local organizations
- 9 higher-ed institutions
- 9 K-12 school districts
- 1 tribal entity
- 1 federal agency

Learn more at: Participating Governments

As Cyber Threats Grow, How Do Governments Know…

If a cloud solution that is being used to deliver services that transmit, store and/or process your data ***could impact security***?

If bidders meet minimum security standards ***before*** making an award for contract?

If a contracted product complies with your security standards ***throughout the duration of the contract***?

GovRAMP (Gov Risk Authorization Management Program)

Who they are:

- A 501(c)(6) nonprofit membership organization (formerly StateRAMP) that supports state, local, federal, educational, tribal, and nonprofit organizations **in securely adopting cloud technologies**.
- A Government Engagement Team (GET) and Program Management Office (PMO) working to **advance cybersecurity standards and procurement efficiency** for our participating organizations.

What they do:

- Establish a **standardized, streamlined security verification process** for cloud service providers.
- **Serve as a no-cost, trusted partner for SLED agencies**.
- **Maintain an Authorized Product List** of cloud products that meet GovRAMP's security standards.

How they do it:

- **Leverage NIST 800-53 Rev. 5 framework** to assess and verify security of cloud products.
- Facilitate a **shared security assessment process** to reduce redundancy and increase procurement efficiency.
- **Provide transparency** through continuous monitoring.
- **Support governments** throughout every step of the GovRAMP adoption process.

Which Assessments Work for North Carolina?

Making Waves by Advancing Security

Successive Achievement

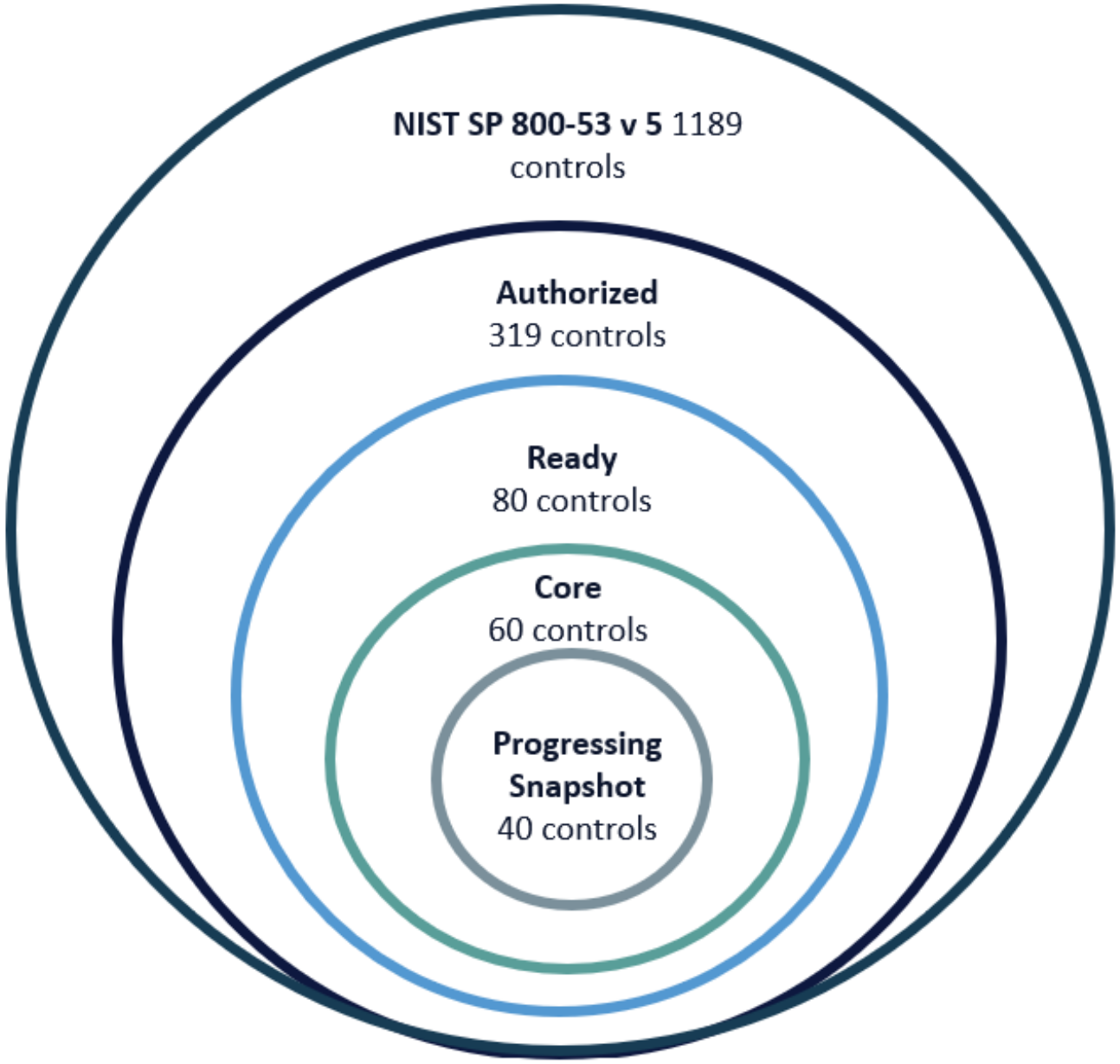
- Each GovRAMP Status builds on the previous and advances the provider to the next status

Focus on Impact

- NIST Control Selection was based on biggest impact per the MITRE ATT&CK Framework Risk Protection Values

Removing Barriers

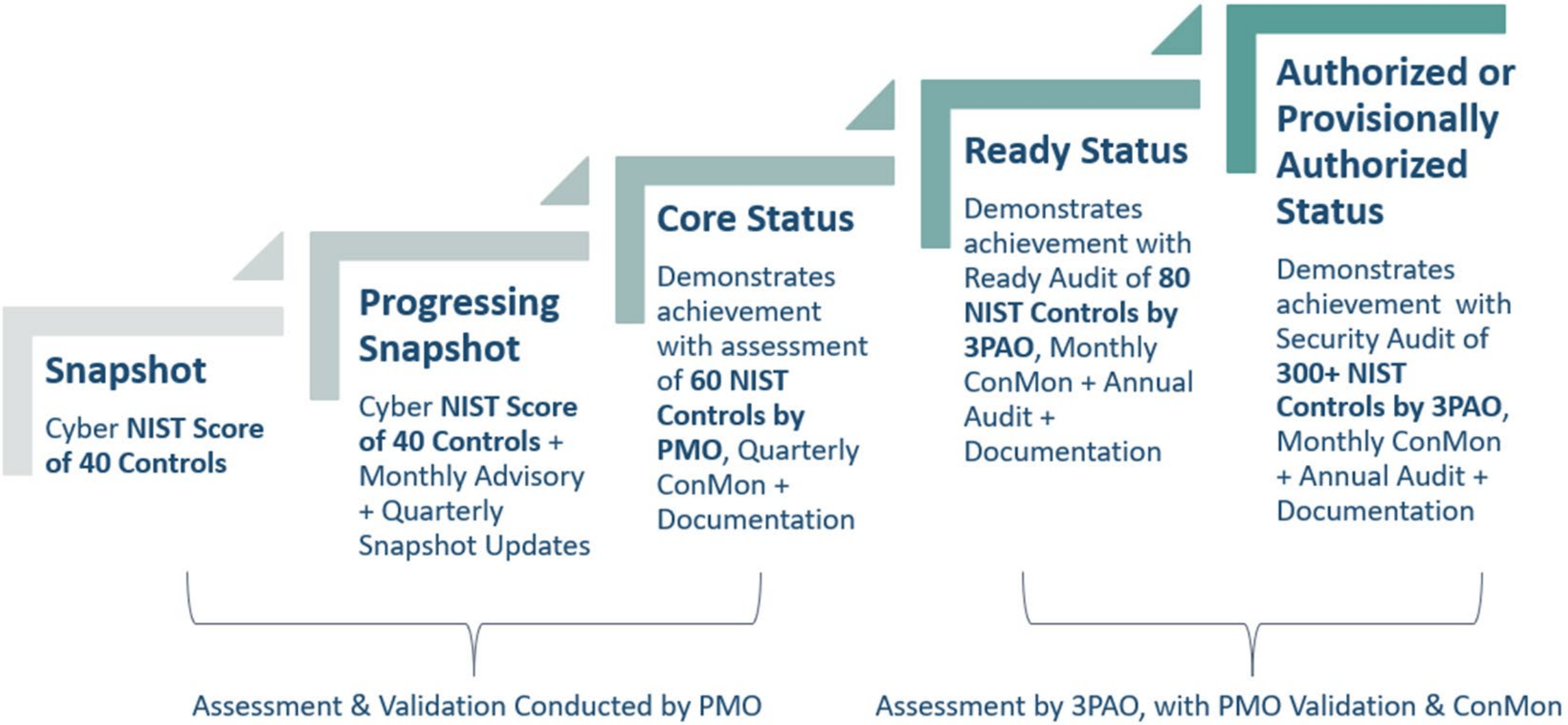
- Service providers often don't know where to start
- GovRAMP Progressing SnapShot and GovRAMP Core have a lower entry cost



GovRAMP's Security Framework & Status

STANDARDIZING AND STREAMLINING THE SECURITY VERIFICATION PROCESS FOR SAFER, MORE EFFICIENT CLOUD PROCUREMENT

GovRAMP Security Statuses



GovRAMP's Security Framework

GovRAMP's baseline requirements are built on NIST 800-53 Rev. 5.

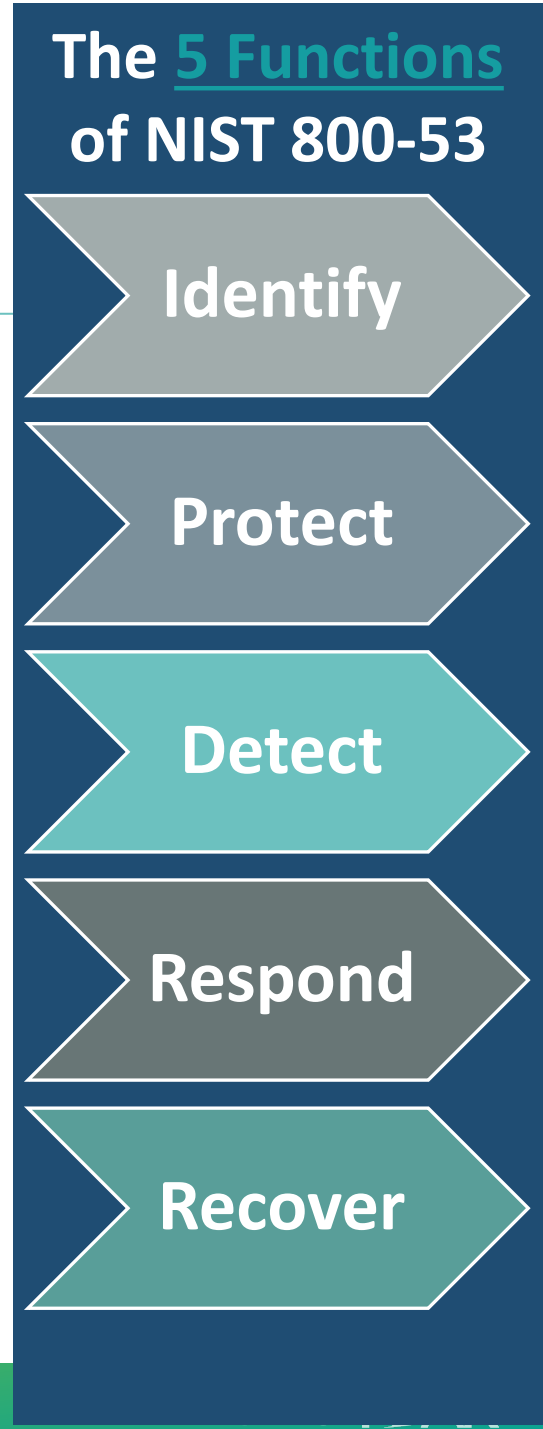
This framework:

- Is modeled after industry best practices
- Easily translates to SLED organizations
- Is applied in the assessment of cloud products that serve public sector organizations

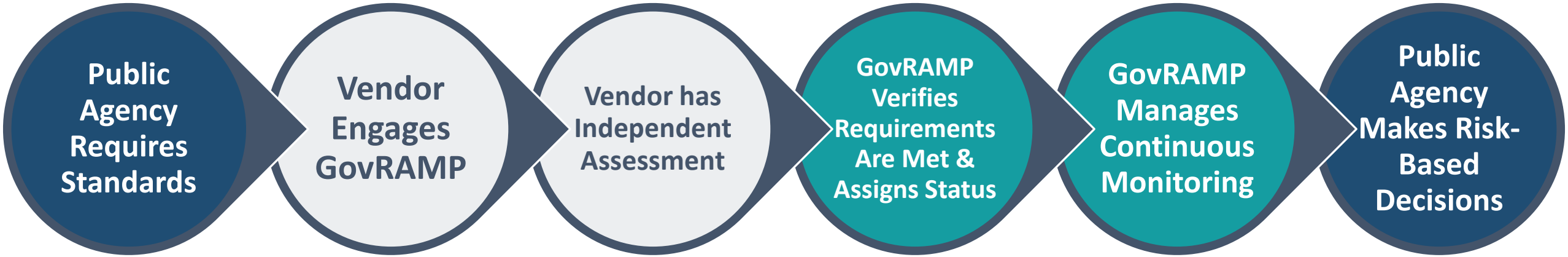
GovRAMP's governance committees adopt policies that define:

- Baseline minimum standards
- Processes for GovRAMP verification

Find policies, templates and resources online at:
GovRAMP.org/templates-resources



GovRAMP: Trust but Verify for Secure Procurement



What This Means for Procurement Entities:

- You no longer need to collect a Vendor Readiness Assessment Review (VRAR) for Vendor Hosted Solutions during the initial phases of an IT procurement (you will still need to do that for **state hosted** solutions **at this time**)
- You no longer need to to collect Third Party Attestations (TPA) to forward to your security team for review prior to award (e.g. Soc 2 Type 2, ISO 27001 and/or HISTRUST, etc.) for solutions hosting **restricted** data.
- Because of Continuous Monitoring (ConMon) by GovRAMP, you no longer need to collect Standards Exceptions for hosting initially or annually.
- This doesn't entirely replace what your security departments do: API's and connections to/from state infrastructure are still closely analyzed.

To Summarize for Vendor Hosted Solutions:

- No VRAR's need to be collected
- No Third Party Attestations (e.g. Soc 2 Type 2, ISO 27001 and/or HISTRUST, etc.) need to be collected
- No Hosting Exceptions initially or annually
- You will have to collect and have your security team confirm that the vendor has the appropriate GovRAMP certification for your procurement/application/solution prior to award. That would (or should) be collected at offer submittal but is a must prior to award.
- Vendors have one (1) year to transition to this new security standard and IT templates and terms will be updated once the new method goes into effect.

Scope of New GovRAMP Requirements

- **In scope:**
  - Third-party external cloud services utilized by the state of North Carolina
  - New cloud contracts/solicitations, effective April 1
  - Existing contracts up for renewal – at time of new solicitation
- **Out of scope:**
  - On-premises systems and solutions
  - Cloud products that are currently under contract and not up for renewal
- North Carolina will implement a **one-year on-ramp period**, **from April 1, 2026 – April 1, 2027**, to allow vendors time to meet requirements.
- In order for a bid to be accepted, the proposed product will need to be GovRAMP or FedRAMP engaged unless otherwise instructed by North Carolina.
- For cloud services procured through the SITP process, NCDIT will also participate in the annual review and validation.

Continuous Monitoring

Ready, Authorized, or Provisionally Authorized Statuses

- **Monthly vulnerability reporting and POA&M** update from provider to GovRAMP PMO
- **Annual assessment by 3PAO** submitted to PMO
- **Monthly reporting** from PMO to participating governments

Core Status

- **Quarterly vulnerability reporting and POA&M update** from provider to GovRAMP PMO
- **Quarterly reporting** from PMO to participating governments

- **Designated staff will have access to view contracted CSP's security packages on GovRAMP's Continuous Monitoring portal.**
- Providers must comply with Continuous Monitoring (ConMon) requirements to maintain the status of Core, Ready, Authorized or Provisionally Authorized.
- View GovRAMP policies that establish our security standards & requirements: GovRAMP.org/templates-resources

Authorized Product List

Verified and Progressing Products are listed on the Authorized Product List and updated daily.

- Our Authorized Product List is a public list on govramp.org/product-list/
- Section 1: Ready, Authorized, Provisionally Authorized Product
  - Total Products: 135+
- Section 2: Progressing Snapshot Program, Active, Pending, In Process Products
  - Total Products: 190+
- Continuous monitoring is required to maintain a verified listing of Core, Ready, Authorized and Provisionally Authorized

Participating GovRAMP Governments can be provided secure access to GovRAMP portal to view continuous monitoring upon provider approval.

North Carolina's GovRAMP Implementation

North Carolina GovRAMP Adoption

- North Carolina is committed to starting a phased rollout of GovRAMP, beginning April 1. Only GovRAMP or FedRAMP Rev. 5 will be accepted.
- North Carolina will implement a one-year on-ramp period, from April 1, 2026 – April 1, 2027, to allow vendors time to meet requirements.
- An updated **Third-Party Cloud Service Risk Authorization & Management Statewide Information Security Manual Supplement** has been published, outlining the new GovRAMP requirements for third-party external cloud services.
- An updated **Statewide Data Classification and Handling Policy** has been published, effective April 1, 2026.
- Register for the next agency webinar:
  - April 21: 2 – 3 PM ET | **Register**

Interim GovRAMP Monitoring Requirement Process

- **Applicable for Internal, Confidential and Restricted data. Does not apply to Public Data.**

- If a chosen CSP does not hold the required GovRAMP status (Core, Ready or Authorized) prior to contract award, the CSP has the option to achieve that status within a set interim timeframe. N.C. agencies must follow these monitoring requirements to safeguard data:
  - Prior to contract award, agencies are responsible for reviewing GSSS.
  - Once the contract is awarded, agencies must confirm enrollment in the GovRAMP **Progressing Snapshot Program (PSP)** PRIOR to any non-public state data being transferred to, stored in, or processed by the cloud service.
  - For CSPs processing Confidential and/or Restricted information, agencies must validate Progressing Snapshots quarterly in accordance with existing data handling requirements.

Interim GovRAMP Monitoring Requirement Process (cont.)

- **Extensions:**
  - **Applicable for Internal, Confidential and Restricted data. Does not apply to public data.**
  - If the CSP is not able to obtain the required status (Core, Ready, or Authorized/Provisionally Authorized within the given interim time frame (Core – 12 months, Ready – 15 months, Authorized – 21 months), **extensions may be granted at the discretion of the purchasing state agency**, provided that the Security Liaison has reviewed the most recent Progressing Snapshot and has validated that the appropriate mitigations are in place to protect state data.
  - **Extensions may not exceed six (6) months.**
  - If the CSP is in the authorization queue for the appropriate GovRAMP status but is not yet formally authorized, state agencies may accept a GovRAMP PMO letter indicating that the product is currently in the process of being reviewed for a verified status.

FedRAMP Reciprocity

- If the cloud service holds a **FedRAMP Rev. 5 authorization** at time of award, this authorization can be accepted in lieu of a GovRAMP authorization.
- Authorizations obtained via the **FedRAMP 20x Pilot Program** will ***not*** be permitted.
- Agencies are responsible for validating at least annually via the FedRAMP Marketplace or equivalent attestation that the cloud service's FedRAMP authorization is in good standing.
- For cloud services procured through the SITP process, NCDIT will also participate in review and validation.
- State agencies may identify a business need to require a cloud service to enroll in the **GovRAMP Fast Track program**.
  - When this is required, agencies are responsible for validating that the CSP has enrolled in the GovRAMP Fast Track program to achieve a status of GovRAMP Authorized or Provisionally Authorized.

Contact Information

- For North Carolina inquiries: **ESRMO@nc.gov**
- For GovRAMP inquiries: **Amy@govramp.org**
- North Carolina GovRAMP webpages:
  - **The State of North Carolina & GovRAMP**
  - **GovRAMP Adoption | NCDIT**
- Register for the next agency webinar:
  - April 21: 2 to 3 p.m. EST | **Register**
- Register for the next vendor webinars:
  - Wednesday, April 22: 3 to 4 PM EST |**Register**
- Sign up for GovRAMP's **Biannual Education Series** on September 16

Stay Connected with GovRAMP

GovRAMP Resources

- GovRAMP Homepage
- GovRAMP Memberships
- Participating Governments
- REV 5 Templates and Resources
- Data Classification Tool
- Cloud Procurement Resource Tool
- Authorized Product List
- Security Assessment Framework
- **Communications & Events**
  - GovRAMP Blog
  - Sign up for GovRAMP Communications
  - Upcoming GovRAMP Events
  - LinkedIn

Questions?

THANK YOU!

Optional Slides if there is time after Q&A

THESE GO DEEPER TECHNICALLY AND I DON'T BELIEVE THE PROCUREMENT FOLKS WOULD BE INTERESTED OR FOLLOW.

Public Data (formerly low-risk)

- **Public Data**: data that is open to public inspection according to state and federal law, state policy, or readily available through public sources (e.g., information on publicly accessible websites, work email addresses, etc.)

- Where the highest category of information to be processed is public, N.C. agencies must:
  - **Validate the applicable GovRAMP Security Snapshot Score (GSSS) *prior* to contract award**. Sample GSSS and Snapshot Matrix.
  - **Review an updated GSSS annually throughout contract duration** to validate that the CSP is meeting or exceeding their original contracted score.

- Products with GovRAMP Core, Ready, Authorized or Provisionally Authorized statuses or FedRAMP Rev. 5 authorization also satisfies the security requirement.

Internal Data (formerly part of medium-risk)

- **Internal data**: information that most state agency employees would have access to, but that is not meant to be shared with the public (e.g., draft documents that have not yet been published, employee work schedules, internal newsletters, training materials, etc.).

- Where the highest category of information to be processed is internal, N.C. agencies must:
  - **Validate that the CSP has achieved the status of GovRAMP Core prior to award**, or;
  - *Follow the on-ramp/Interim GovRAMP Monitoring Requirement Process in Slides 13 & 14*
    - **Validate that the CSP has agreed to achieve GovRAMP Core status within an interim time period**, no later than twelve (12) months from the date of contract.

- Products with GovRAMP Ready, Authorized, or Provisionally Authorized statuses or FedRAMP Rev. 5 authorization also satisfies the security requirement.

Confidential Data (formerly part of medium-risk)

- **Confidential data**: information that is limited to a small audience with a need-to-know or legitimate business case (e.g., state employee personnel records, trade secrets, student records, sensitive public security information, etc.). If exposed to unauthorized parties, there will be high impact consequences such as regulatory fines, inability to recruit talent, loss of confidence, and/or damage to vendor relationships.
- Where the highest category of information to be processed is confidential, agencies must:
  - **Validate that the CSP has achieved the status of GovRAMP Ready prior to award**, or;
  - *Follow the on-ramp/Interim GovRAMP Monitoring Requirement Process in Slides 13 & 14*
    - **Validate that the CSP has agreed to achieve GovRAMP Ready status within an interim time period**, no later than fifteen (15) months from the date of contract.
- Products with GovRAMP Authorized or Provisionally Authorized statuses or FedRAMP Rev. 5 authorization also satisfies the security requirement.

Restricted Data (formerly high risk)

- **Restricted data**: represents the highest risk to the state, state agencies, and constituents if it is disclosed or compromised. Likely regulated by law and access to it is restricted to a limited audience (e.g., State and Federal Tax Information [FTI], Payment Card data, Protected Health Information [PHI], Criminal Justice Information [CJI], SSA, etc.).
- Where the highest category of information to be processed is restricted, N.C. agencies must:
  - **Validate that the CSP has achieved the status of GovRAMP Authorized prior to award**, or;
  - *Follow the on-ramp/Interim GovRAMP Monitoring Requirement Process in slides 13 & 14*
    - **Validate that the CSP has agreed to achieve GovRAMP Authorized status within an interim time period**, no later than twenty-one (21) months from the date of contract.
- If the CSP stores, processes, or transmits criminal justice data, it may be required to achieve Authorized/Provisionally Authorized status with the **CJIS Aligned Overlay.**