Understanding GovRAMP: An Overview for North Carolina Vendors

March 16, 2026

Agenda

- What is GovRAMP?
- GovRAMP Security Framework and Statuses
- North Carolina’s GovRAMP Implementation
- Q&A

What is GovRAMP?

CREATING A FRAMEWORK FOR CONTINUOUS IMPROVEMENT IN CYBERSECURITY FOR NORTH CAROLINA, ITS PROVIDERS, AND THE CONSTITUENTS THEY SERVE.

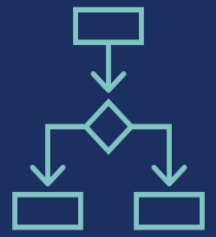
GovRAMP (Gov Risk Authorization Management Program)

Who we 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 we do:

- Establish a **standardized, streamlined security verification process** for cloud products (IaaS, SaaS, & PaaS).
- **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 we 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** in adopting GovRAMP and **support vendors** during the security verification process.

GovRAMP's Security Framework & Statuses

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

GovRAMP's Security Framework

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

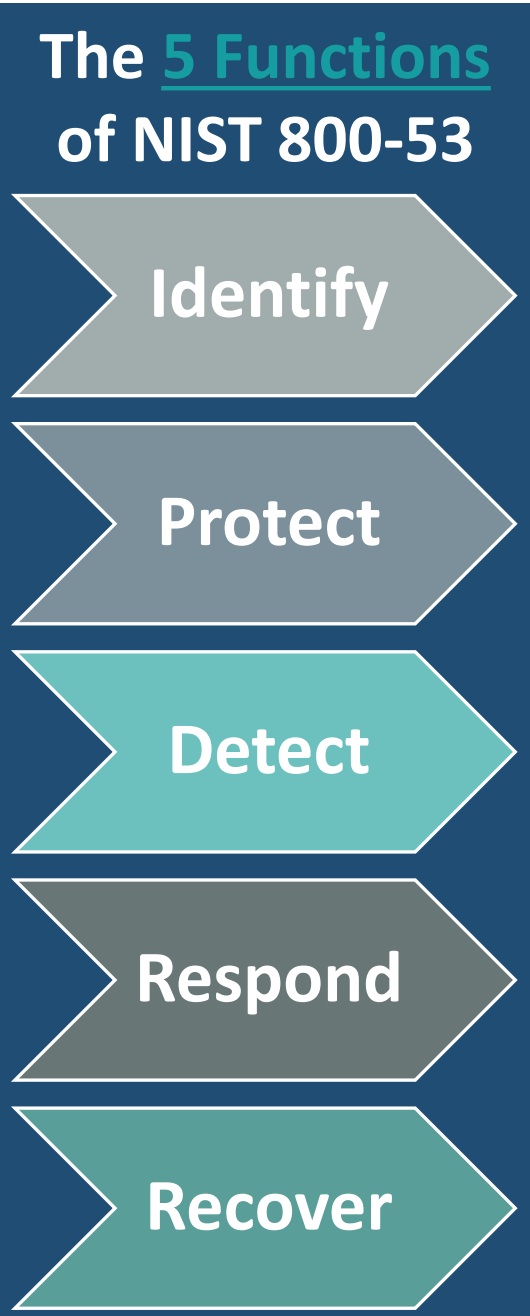
This framework:

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

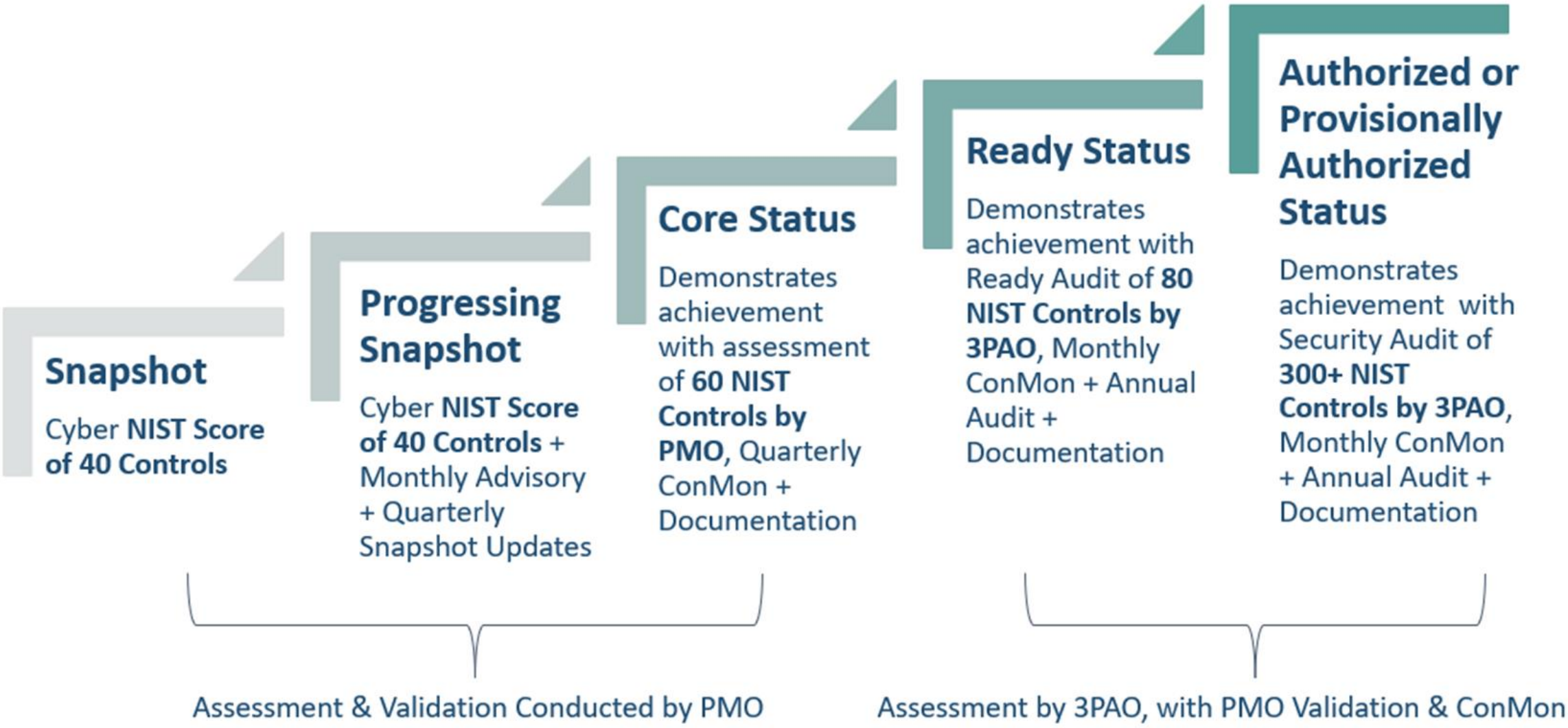
GovRAMP's governance committees adopt policies that define:

- Baseline minimum standards
- Processes for GovRAMP verification

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



GovRAMP Security Statuses



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

Providers must comply with Continuous Monitoring (ConMon) requirements to maintain the status of Core, Ready, Authorized, or Provisionally Authorized.

Providers may grant viewing access to Participating Governments at the Standard Access level or the Elevated Access level.

View GovRAMP policies that establish our security standards & requirements: GovRAMP.org/templates-resources

Single Snapshot – 40 NIST controls

- Receive a product security maturity score approximately 3 weeks after submitting required documentation

Progressing Snapshot – 40 NIST controls

- Ongoing program with quarterly snapshots

Core – 60 NIST controls, 12 months to achieve from contract award

- Quarterly continuous monitoring requirements

Ready – 80 NIST controls, 15 months to achieve from contract award

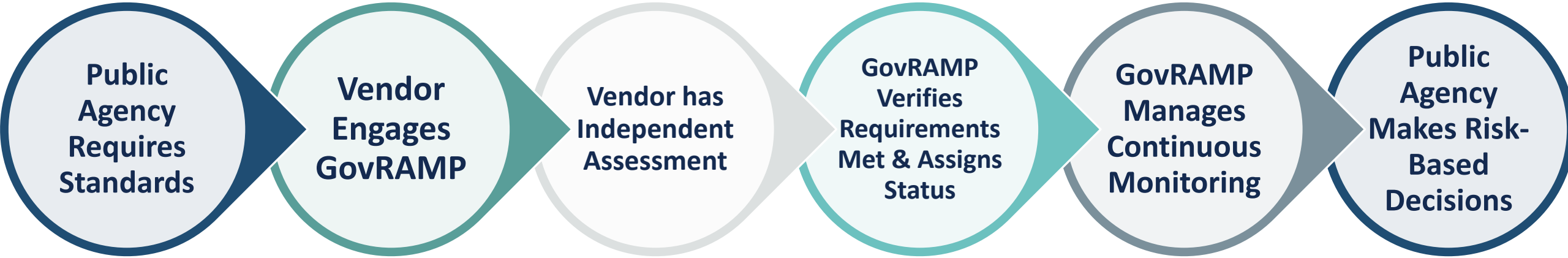
- 3PAO assessment, PMO annual assessment, and monthly continuous monitoring requirements
- GovRAMP Fast Track Option if the product has or is pursuing FedRAMP Rev. 5 authorization

Authorized/Provisionally Authorized – 300+ NIST controls, 21 months to achieve from award

- 3PAO assessment, PMO annual assessment, and monthly continuous monitoring requirements
- Requires approval from an authorizing government official – sponsorship or GovRAMP Approvals Committee
- GovRAMP Fast Track Option if the product has or is pursuing FedRAMP Rev. 5 authorization
- CJIS Aligned Overlay available

- Progressing Snapshot: **Progressing Product List**. Core, Ready, & Authorized: **Authorized Product List**
- **GovRAMP Fee Schedule**

High-Level GovRAMP Process



North Carolina's GovRAMP Implementation

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 at the time of bid** unless otherwise instructed by North Carolina.

North Carolina GovRAMP Adoption

- North Carolina is committed to starting a phased rollout of GovRAMP, beginning April 1. **Only GovRAMP or FedRAMP Rev. 5 engaged-products 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.
- The ***Third-Party Cloud Service Risk Authorization & Management Statewide Information Security Manual Supplement*** (SISM 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 vendor webinar on Wednesday, April 22 from 3 – 4 PM ET|**Register**

Reciprocity: Not Accepted (including but not limited to)

The following will not be accepted:

- SOC 2
- ISO 27001
- HITRUST

Reason for Non-Acceptance

The 2018 National Cyber Strategy of the USA identifies NIST as the only Cybersecurity Framework (CSF) for assessing SaaS, PaaS, or IaaS vendor environments.

The State of North Carolina is not accepting any other form of CSF for this assessment including but not limited to self-attestations, trust documents, third-party assessments to include COBIT, ISO/IEC 27000 series, PCI, SOC 2 or SOC 3 reports.

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.
- North Carolina State Agencies may identify a business need to require a cloud service to enroll in the **GovRAMP Fast Track program**.
  - When this is required, the CSP must enroll in the GovRAMP Fast Track program to achieve a status of GovRAMP Authorized or Provisionally Authorized.

New Contracts

- New Requirements begin April 1, 2026, for new solicitations/contracts
- **In order to participate and an offer be accepted, the proposed product will need to be GovRAMP or FedRAMP engaged at the time of bid unless otherwise instructed by North Carolina**
- GovRAMP requirements are correlated to the data classification level, as determined by the soliciting agency and as detailed in the **Statewide Data Classification and Handling Policy** and the **SISM Supplement**. These requirements will be detailed in each individual solicitation.
- North Carolina has classified four data types – Public, Internal, Confidential, and Restricted.

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, at the time of bid, a vendor must:
  - **Submit GovRAMP Security Snapshot Score (GSSS) *prior* to contract award**. Sample GSSS.
  - **Submit an updated GSSS annually throughout contract duration**, with a score meeting or exceeding the original contracted score.

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

Interim (On-Ramp) Vendor GovRAMP Process

- **Applicable for Internal, Confidential, & Restricted data. Does not apply to Public Data.**
- **Applicable only from April 1, 2026 – April 1, 2027 (on-ramp period).**
- If a product does not hold the required GovRAMP (Core, Ready, or Authorized) or FedRAMP Rev. 5 status prior to contract award, the CSP has the option to achieve that status within a set timeframe. In order to satisfy security requirements, vendors must:
  - Submit a GSSS at the time of bid.
  - Once the contract is awarded, enroll in the GovRAMP **Progressing Snapshot Program (PSP)** PRIOR to any non-public State data being transferred, stored, or processed.
  - For CSPs processing Confidential and/or Restricted information, submit Progressing Snapshots quarterly.
  - Commit to achieving the required status within the established timeframe.

Internal Data (formerly part of medium-risk)

- **Internal data**: information that most State 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, a vendor must:
  - **Achieve the status of GovRAMP Core prior to contract award**, or;
  - *Follow the on-ramp/Interim GovRAMP Monitoring Requirement Process in Slide 18 as follows:*
    - **Provide a GovRAMP Security Snapshot Score at bid**
    - **Enroll in the GovRAMP Progressing Snapshot Program**
    - **Agree to achieve GovRAMP Core status** 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 satisfy 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., employee records, sensitive public security information, etc.). Unauthorized exposure would lead to 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, a vendor must:
  - **Achieve the status of GovRAMP Ready prior to award**, or;
  - *Follow the on-ramp/Interim GovRAMP Monitoring Requirement Process in Slide 18 as follows:*
    - **Provide a GovRAMP Security Snapshot Score at bid**
    - **Enroll in the GovRAMP Progressing Snapshot Program**
    - **Agree to achieve GovRAMP Ready status** 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 satisfy the security requirement.

Restricted Data (formerly high-risk)

- **Restricted data**: highest risk to the State if data is disclosed or compromised. Regulated by law and access is restricted audience (e.g., Tax Information, Payment Card data, Protected Health Information [PHI], Criminal Justice Information [CJI], SSA, etc.).
- Where the highest category of information to be processed is restricted, a vendor must:
  - **Achieve the status of GovRAMP Authorized prior to award**, or;
  - *Follow the on-ramp/Interim GovRAMP Monitoring Requirement Process in Slide 18*
    - **Provide a GovRAMP Security Snapshot Score at bid**
    - **Enroll in the GovRAMP Progressing Snapshot Program**
    - **Agree to achieve GovRAMP Authorized status within an interim time period**, no later than twenty-one (21) months from the date of contract.
- Products with FedRAMP Rev. 5 authorization also satisfy the security requirement.
- 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.**

Summary of Requirements by Data Classification
(on-ramp period applicable through April 1, 2027)

Public Data

- Submit GSSS at bid and annually; or
- Hold GovRAMP Core, Ready, Authorized, or Provisionally Authorized or FedRAMP Rev. 5 Authorization status

Internal Data

- GovRAMP Core; or
- GSSS at bid, enroll in PSP, and commit to Core in 12 months, or;
- Hold GovRAMP Ready, Authorized, or Provisionally Authorized or FedRAMP Rev. 5 Authorization status

Confidential Data

- GovRAMP Ready, or;
- GSSS at bid, enroll in PSP, and commit to Ready in 15 months, or;
- Hold GovRAMP Authorized or Provisionally Authorized or FedRAMP Rev. 5 Authorization status

Restricted Data

- GovRAMP Authorized/Provisionally Authorized
- GSSS at bid, enroll in PSP, and commit to Authorized/Provisionally Authorized in 21 months, or;
- Hold FedRAMP Rev. 5 Authorization

- See individual slides and the ***Third-Party Cloud Service Risk Authorization & Management Statewide Information Security Manual Supplement*** (SISM Supplement) and ***Statewide Data Classification and Handling Policy*** for more details.
- As of April 1, 2027, vendors must hold the required GovRAMP status or FedRAMP Rev. 5 Authorization at the time of bid in order to be awarded a contract.

Timeline Overview

New Contracts: April 1, 2026

On-ramp period: April 1, 2026 – April 1, 2027

Existing Contracts (not up for renewal): At point of new solicitation

Note: Effective April 1, 2027, all solicitations with a requirement of GovRAMP verified status of Core, Ready, or Authorized/Provisionally Authorized or FedRAMP will require that the product already hold the required verified status at the time of bid.

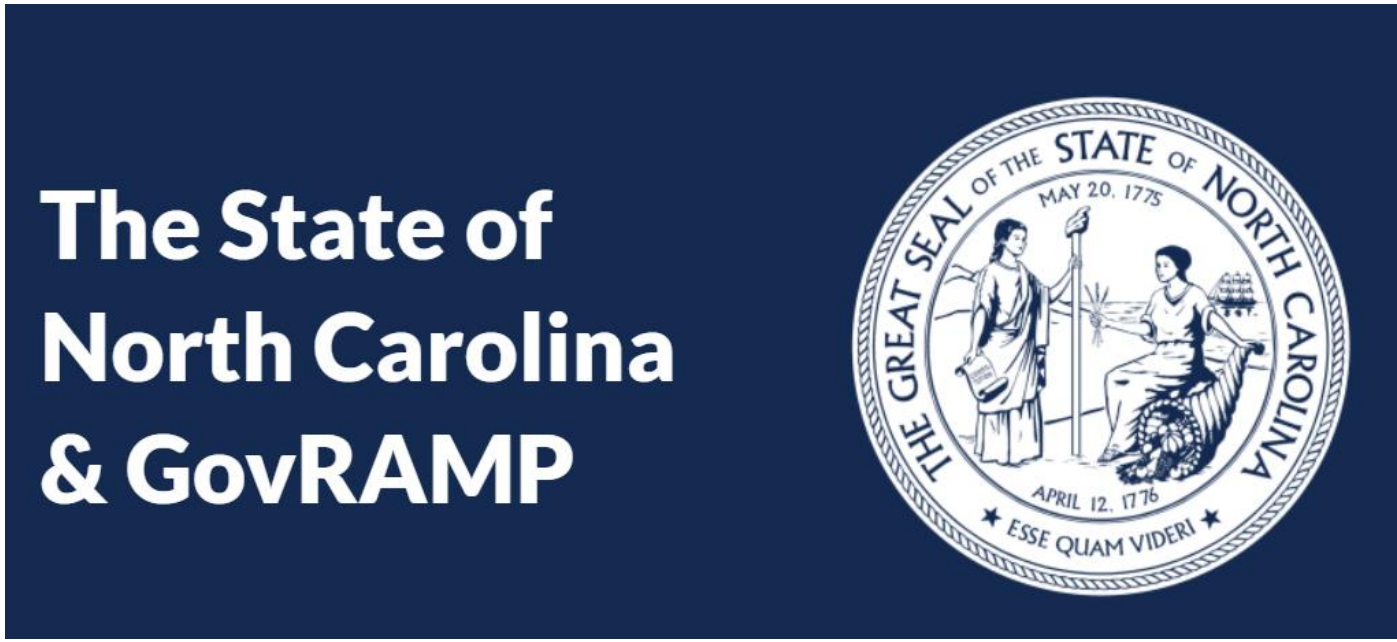
Next Steps

- **Be proactive!**
- Bookmark **North Carolina's GovRAMP page** so that you are always up to date.
- Review trainings posted on the NC Program Page – this recording will be posted within a week.
- Keep an eye out for future trainings & Office Hours.
- Download the GovRAMP provider **templates** and decide which path works best for you while still meeting North Carolina's requirements.
- Contact GovRAMP at **info@govramp.org** to meet your assigned Cyber Solutions Specialist.

State of North Carolina & GovRAMP Webpages

- **State of North Carolina GovRAMP Program Page**
  - Communications
    - Announcements
    - Document Library
    - Training Library
    - Points of Contact
    - GovRAMP Requirements
    - Links to Resources

- **North Carolina webpage**



Contact Information

- For North Carolina related inquiries: **ESRMO@nc.gov**
- For GovRAMP-related inquiries: **info@govramp.org** or **Amy@govramp.org**
- North Carolina GovRAMP webpages:
  - **The State of North Carolina & GovRAMP**
  - **GovRAMP Adoption | NCDIT**

Stay Connected with GovRAMP

Get Started by Joining the Mission

- Once membership is confirmed, each provider will be assigned a RAMPQuest Account Manager.
- Email info@govramp.org

Become a Member at
govramp.org/memberships

Membership Benefits

Have a Voice	Nominate for Committee	Provider Leadership Council	Access GovRAMP Program	Education & Resources	Improve Nation's Security!

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!

Appendix

THANK YOU!

GovRAMP Program Offerings

SINGLE SNAPSHOT

The **evidence-based** GovRAMP Security Snapshot helps service providers start their cybersecurity journey, while offering governments a first look at cloud products' risk maturity. It validates the product's maturity by examining the top 40 most impactful controls determined by MITRE's ATT&CK® Framework as the basis. The Security Snapshot is valid for a period of 12 months from the date of issuance and may be leveraged by multiple organizations during that time period.

PROGRESSING SNAPSHOT

A major goal of the GovRAMP Progressing Security Snapshot Program is enhancing cyber maturity among providers and fostering information sharing that facilitates effective government risk management by integrating the principles of "trust but verify" and a consultative approach.

The program includes quarterly assessments (Snapshots) and monthly consultative calls with the GovRAMP PMO Advisory team. Service providers gain insight into their products' gaps in achieving NIST-based security controls and guidance on how to best address those gaps, with a focus on what matters most for improved security outcomes.

GovRAMP Program Offerings

CORE

Achievable in 12 Months

The GovRAMP Core security status provides an early step in verified GovRAMP statuses to demonstrate the maturity of a cloud product's security program. This early step demonstrates achievement of baseline NIST 800-53 Rev. 5 controls and documentation requirements as assessed and validated by the GovRAMP PMO. The provider may optionally submit a Pen Test. Like other GovRAMP verified statuses, the Core Status is valid for 12 months and may be extended for an additional 12 months by undergoing an annual assessment prior to the status expiration. There is no limit to the number of extensions a product may obtain.

To maintain a GovRAMP Core security status, the provider must comply with quarterly continuous monitoring requirements that include submission of evidence of Core requirement compliance as requested by the GovRAMP PMO, in addition to Web App Scans, Vulnerability Scans, Policy Compliance Scans and a POA&M spreadsheet.

READY

Achievable in 12-18 Months

A Ready status indicates that the product meets GovRAMP's Minimum Mandatory Requirements and most critical controls. The Ready requirements are published here and vary by Impact Level for Low, Moderate, or High. The security package for Ready includes a Readiness Assessment Report (RAR) submitted by a GovRAMP 3PAO, attesting to the minimum mandates. The required Ready documentation, including boundary diagram, inventory worksheet, roles, and permissions matrix, must be included in the security package provided to our Security Team through the GovRAMP Program Management Office (PMO). The GovRAMP PMO provides independent validation and verification that the security package and RAR comply with the standards established by the GovRAMP governing board and committees.

GovRAMP Program Offerings

PROVISIONALLY AUTHORIZED

Achievable in 18-24 Months

A Provisionally Authorized status may be assigned by a sponsoring government or Approvals Committee to a package submitted for Authorized Status, if the product meets the Authorization requirements, but one of the product's interconnected technologies is not GovRAMP or FedRAMP Authorized. To achieve Provisionally Authorized, the interconnected technology must leverage a current GovRAMP Security Snapshot.

AUTHORIZED

Achievable in 18-24 Months

An Authorized Status indicates the product or offering meets all the required NIST controls by impact level and the provider has completed the necessary documentation, including a 3PAO Security Assessment Report. To obtain Authorized status, a security package needs approval from the Approvals Committee or a Government Sponsorship. They will serve as authorization officials and confirm the package meets GovRAMP requirements.

GovRAMP and FedRAMP

Join the GovRAMP Working Group to learn more: govramp.org/working-group/

	GovRAMP	FedRAMP
Based on NIST 800-53 Rev. 5	✓	✓
Requires annual independent 3PAO assessment	✓	✓
Requires Monthly Continuous Monitoring	✓	✓
Impact Levels of Low, Moderate, and High	✓	✓
Verified statuses of Ready and Authorized	✓	✓
Available to any provider, regardless of federal contract status	✓	
Documentation available to federal, state, local, public education institutions, and special districts	✓	
Centralized PMO reviews all security packages to ensure consistent application of standards and verification	✓	
Fast Track option for products with FedRAMP or GovRAMP	✓	
Plans for mapping to other compliance frameworks: CJIS, MARSE, MMIS, IRS	✓	
Nonprofit mission to improve cyber posture for SLED organizations and providers who serve them	✓	

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.

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