Navigating Challenges: How GovRAMP Empowers State and Local Governments

It may be easy to think of the state and local market as the smaller sibling of the federal government—but in reality, state and local agencies are far more complex than their federal counterparts. Their scope is vast, encompassing responsibility for education, healthcare, infrastructure, transportation, public safety, and even hunting and fishing. While these are also concerns at the federal level, the federal agencies responsible for each area are well-defined and operate fairly independently. State and local governments, on the other hand, tend to share diverse responsibilities (as well as shared budgets) across organizations.

This diversity does not exist only within a state but across the market. Some states are better funded than others, and large cities have bigger pools of resources than small towns. Even with this in mind, there are some common challenges that can be defined market-wide. There are also common solutions that can help solve these challenges no matter the size or location of the localized agency. This is where GovRAMP has proven to be an invaluable resource in helping state and local agencies modernize their IT as well as their practices.

This report, in examining key challenges, looks at how state and local agencies procure and utilize modern technologies to serve their citizens.

Challenge 1: Budget

State and local budgets are funded through a combination of tax revenue and federal investments. In today's political and economic climate, both sources are very uncertain. If a state is not growing quickly, its revenue, and as a result, its budget, shrinks. States cannot count on federal investment to help bridge slow local economies.

Faced with tight budgets, states and localities often have to make difficult choices: invest in new technology to support IT modernization goals, or ensure that school lunches remain fully funded. "These trade-offs force state and local organizations to be ruthlessly selective," says Morgan Reed, SLED Field CTO at Okta. "Every solution must meet mission needs both affordably and securely."

Zach Oxman, area vice president for Abnormal AI, points out that in this "do more with less" environment, states and localities are under pressure to introduce artificial intelligence (AI) for increased efficiency—but to do so, they must understand the technology and its security implications.

Challenge 2: Security

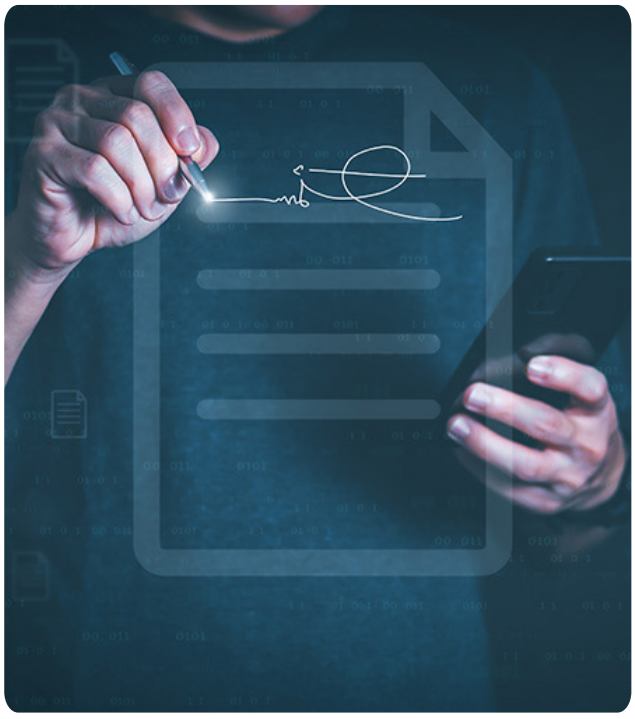
State and local agencies are top targets for cyber threats due to the value of the personal data they hold and the criticality of their mission. Add to that bad actors' knowledge that these groups are underfunded when it comes to technology and cybersecurity, and you have the perfect storm. In 2024 alone, 34% of state and local entities reported a ransomware attack.

> " With Generative AI [Gen AI], bad actors are moving to social engineering as the dominant way to attack. "
>
> - Zach Oxman, Abnormal AI

With Gen AI, phishing emails can be made to look more realistic than ever and can be quickly created in larger batches, overwhelming an organization. He points out that with so much government business (e.g., meeting minutes, memos) published online, all the content bad actors need to create realistic communications is readily available.

Similarly, Gen AI is allowing bad actors to more easily and quickly create spoofed accounts for benefits fraud, adds Matt Conner, chief information security officer with Second Front Systems.

"With so many under-resourced states, we cannot expect a state infrastructure to withstand a nation-state attack," says Conner. Not only do states have to validate their employees, they also have a high volume of interactions with the public. Citizen identities need to be validated quickly and seamlessly to ensure information and benefits are being distributed via legitimate requests. Access to security solutions that are easy to implement and manage is critical for this market.



Challenge 3: Staffing

In addition to complicating security considerations, budget challenges also feed staffing challenges. Limited funds not only make it difficult for state and local agencies to compete with private industry based on salary, but small budgets also mean small teams. Okta's Reed lived this reality firsthand as the former CIO for the State of Arizona. He notes that of the 40,000 people the state employed during his tenure, only 15 were allocated to the cyber team.

The region and size of a state or city also impact the availability of talent. Larger cities typically have a broader pool of IT professionals to recruit from. As Second Front's Conner points out, getting "Silicon Valley talent in the middle of Oklahoma is a challenge."

Reed of Okta offers some suggestions for addressing this challenge.

> " To get needed talent, target people in the beginning of their career, highlighting the unique experience that working for a state or local agency provides for growing an IT career. You'll get motivated people who possess the specific skills the IT organization needs. "
>
> - Morgan Reed, Okta

Challenge 4: Technical Debt

Even with a sufficient number of skilled IT team members, the visibility of the tech itself is still a huge challenge. Many states are decentralized, with agencies running their own IT. When a central authority, like a state CIO, wants to understand statewide risk, they often don't even have a view into what technologies are in use. Unknown systems and legacy technology become targets for bad actors who can infiltrate hidden vulnerabilities and hide within unmonitored environments. "When it comes to enforcing policies, oftentimes the CIO can only ask for agencies to opt in," says Deborah Blyth, executive strategist with CrowdStrike. "They often lack visibility into agency environments and do not have sufficient authority to enforce policies broadly."

To modernize systems, many organizations simply "lift and shift" software to the cloud. However, many of these legacy systems were designed before cloud was omnipresent; as a result, they do not work as expected once in the new environment.

> " Organizations can be disappointed when the cost savings promised by cloud adoption don't materialize. They need to triage their technical debt to understand its impact on the overall cloud solution. "
>
> - Matt Conner, Second Front Systems

Conner draws the comparison, "If you move into a new house and then lay down an old dirty carpet, you're not going to like your new house as much."

When it comes to legacy technology, there is often resistance to modernization efforts. CrowdStrike's Blyth notes that many organizations take an "if it's not broke, don't fix it" approach—a difficult argument to counter, especially when budgets are tight.

Finding the On Ramp for Modernization

Modeled after the Federal Risk and Authorization Management Program (FedRAMP), GovRAMP is designed for service providers who offer cloud solutions to state and local governments. It offers a standardized approach to meeting these agencies' cybersecurity requirements. Vendors that become authorized under GovRAMP have demonstrated they meet the baseline security standards defined by the National Institute of Standards and Technology (NIST).

The common baseline defined by GovRAMP enables:

- consistent vendor evaluation for every state and local agency, regardless of agency size or in-house technical expertise;
- reduced ambiguity around what constitutes an acceptable level of security for both buyers and vendors;
- a clearer risk posture, removing the need to create security evaluations from scratch or rely solely on vendor claims;
- faster procurement via an "authorize once, use many times" approach;
- and better threat and risk information sharing, due to a common language and common security thresholds across local, state, and federal entities.

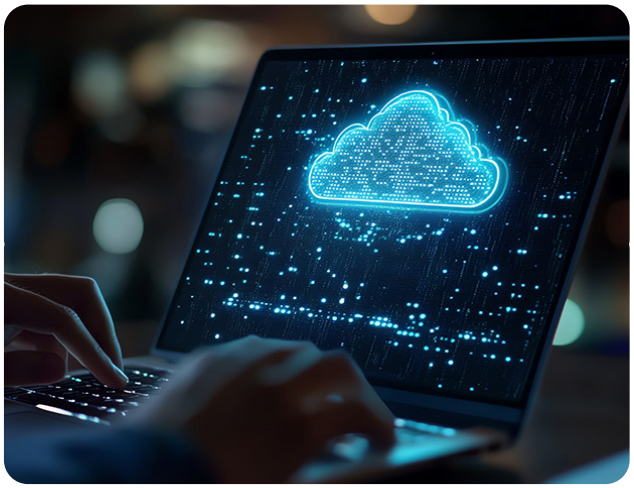
Since GovRAMP is based on the same principles as FedRAMP, companies that are FedRAMP compliant have an easier path to becoming GovRAMP compliant. Blyth points out, however, that unlike FedRAMP, GovRAMP is applicable to non-federal entities and provides assurances to state and local agencies, allowing them to rely upon GovRAMP documentation as evidence of the security of that cloud environment.

Cloud's Link to Security

All of the experts we spoke with agree that GovRAMP has accelerated state and local use of cloud. This has had a huge impact on the uptime of critical applications, points out Reed of Okta. With IT organizations having to focus less on ensuring uptime, their attention can shift to security.

One factor improving security is that cloud solutions incorporate best practices of tech giants (and smaller companies) that have dedicated and fully funded security teams. Additionally, the standardization of security measures means the short-staffed IT and security teams in agencies do not have to personally vet every technology they want to buy and deploy, nor do they have to continually manage the security controls that are part of the cloud solutions. This leaves teams free to focus on the most critical threats and vulnerabilities.

For vendors, GovRAMP's standardization means not having to complete different security requirements and attestations for each state or locality they do business with. Of course, there are some differences in regulations depending on the area, so there will be some variance in requirements, but GovRAMP still gets a vendor most of the way there.



Commitment to the Market

Beyond the promise of secure practices, GovRAMP compliance demonstrates an organization's investment in and understanding of the state and local market. Abnormal AI's Oxman says GovRAMP participation is a sign of an organization's maturity when it comes to security and a commitment to state and local customers.

Earning GovRAMP approval takes time and money, but is worth the investment for companies looking to provide solutions to state and local agencies for the long term. Oxman adds that creating a state-specific version of FedRAMP made the accreditation more accessible to companies that do not have federal customers, removing the need to have a federal-agency sponsor in order to gain proof of compliance.

With that said, CrowdStrike's Blyth suggests that agencies should have alternate methods to acquire technology if a non-GovRAMP provider is what they really need.

> " Organizations may decide that technologies used state-wide should be GovRAMP-certified, while smaller instances within a specific agency could be individually vetted. "
>
> - Deborah Blyth, CrowdStrike

Continuous Monitoring

Like other security standards, including Cybersecurity Maturity Model Certification (CMMC), GovRAMP authorization is not a singular event. GovRAMP vendors must continually demonstrate compliance through regular monitoring and reporting. This work is particularly important given the length of contracts in the public sector space.

Requirements and expectations for ongoing compliance evaluation include:

- regular vulnerability scans
- ongoing Plans of Action and Milestones (POA&Ms) for any identified vulnerabilities or control deficiencies
- submission of regular security package updates
- reporting of certain types of security incidents by affected agencies within defined time windows
- annual assessments by a third-party assessment organization (3PAO) to retest controls and inspect new or changed controls
- automated log collection and security monitoring

Putting this responsibility on the vendor removes the need for agencies to dedicate resources to continuous monitoring, which is especially beneficial for the many SLG agencies that lack the manpower to perform ongoing security oversight. Shifting that onus to the vendor ensures its ongoing compliance and allows the vendor to demonstrate a commitment to meeting the needs of the market.

Ensuring State and Local Agencies Have the Tools Needed to Modernize Securely

Confronted with uncertain budgets, expanding cyber threats, workforce challenges, and significant legacy technology burdens, state and local governments are under pressure to modernize while maintaining uninterrupted delivery of essential public services. In this environment, cloud solutions are a critical enabler, and the use of GovRAMP as a standardized path to acquisition has accelerated cloud use.

GovRAMP's real impact, however, goes beyond compliance. It expands access to modern cloud platforms, shifting agency focus from maintaining uptime to measuring and improving security. It reduces the burden on understaffed cybersecurity teams by allowing them to rely on pre-established controls and automated monitoring. It helps unify fragmented procurement processes across states and localities, increasing efficiency for both agencies and technology providers. And, critically, GovRAMP signals vendor commitment to the long-term needs of the state and local market.

By reducing complexity, strengthening vendor assurance, and expanding access to secure cloud solutions, GovRAMP is positioning agencies to better protect their communities, modernize their operations, and meet the mission-critical demands of today's digital government.

Carahsoft and its partners are committed to helping state, local, and education customers mitigate security risks as they implement cutting-edge technologies to improve service to citizens.

Contact the State and Local Team at Carahsoft to learn more.

GovRAMP@carahsoft.com

SLGmarketing@carahsoft.com

888-662-2724

carahsoft

Explore Carahsoft's portfolio of solutions at:

carah.io/GovRAMP

GovWhitePapers
Where Government Knowledge Gathers

Learn more about GovRAMP on **GovWhitePapers.com**.