THE GROWING DEMAND FOR AGILE, SECURE INFRASTRUCTURE IN GOVERNMENTAL IT

by Anchor Bridge Innovations staff

Across the U.S., public sector agencies are facing increased pressure to modernize outdated IT systems while meeting rigorous security and compliance mandates. This pressure is driving a growing demand for agile, secure infrastructure that can support evolving mission needs.

From local agencies to federal departments, the dual challenge of legacy systems and growing cybersecurity risk is driving urgent demand for modern, cloud-ready solutions. Procurement cycles are accelerating. Compliance frameworks are evolving. And operational expectations are rising — all while budgets remain under scrutiny.

The Current State of Government IT: Burdened by Aging Infrastructure

Despite steady investment, much of the U.S. government's IT ecosystem still relies on outdated systems. According to the Government Accountability Office (GAO), more than **80% of the $100+ billion** annual federal IT spend in FY2024 was allocated to maintaining legacy systems — some more than 30 years old.

And the National Association of State Chief Information Officers (NASCIO) has reported that state governments also struggle with aging infrastructure. In its *State CIO Top Priorities 2024* report, NASCIO lists "legacy modernization" and "cloud services" as the top two IT investment drivers across more than 40 states.

Meanwhile, workforce shortages and funding constraints continue to delay modernization initiatives — creating operational bottlenecks, data silos, and increased exposure to cyber threats.

Cybersecurity Threats on the Rise

The threat landscape has never been more volatile. In 2023, government entities accounted for **14.6% of all reported ransomware incidents** in the U.S., according to IBM's X-Force Threat Intelligence Index 2023. State and local governments remain attractive targets due to their limited cybersecurity staffing and technical debt.

Gartner Inc.'s *Cybersecurity Risk Index for the Public Sector 2024* emphasizes the growing risk of lateral movement attacks enabled by unpatched legacy systems and insufficient identity management controls. Agencies are under increasing pressure to adopt frameworks such as Zero Trust Architecture (ZTA) to stay resilient.

Gartner also noted in its *ZTA Adoption in the Public Sector 2024* that "Government networks, once thought of as static and perimeter-based, now require dynamic, identity-driven access models to stay ahead of threats."

Policy and Compliance Mandates Are Driving Change

Multiple federal mandates and modernization policies are accelerating IT transformation:

- FedRAMP (Federal Risk and Authorization Management Program) mandates that cloud services meet strict security and compliance standards.
- OMB M-22-09 directs agencies to implement a Zero Trust cybersecurity model by FY2027.
- TIC 3.0 (Trusted Internet Connections) provides updated guidance for secure cloud connectivity.

These evolving standards are not just technical guidelines — they are catalysts for funding, cross-agency collaboration, and IT procurement reform.

As *Nextgov/FCW* notes in a 2025 special report, “Compliance is no longer the end goal — it’s the baseline for modernization strategies that align security with agility.”

The Case for Modernization: Agility, Security, and Accountability

Modern infrastructure enables agencies to:

- Scale resources dynamically to support mission needs and citizen services
- Adopt Zero Trust principles and strengthen endpoint security
- Break down silos and enable secure data sharing across agencies
- Reduce technical debt and reallocate budget toward innovation

According to Gartner’s *Public Sector Cloud Adoption Survey 2025*, **69% of agency IT leaders** cite “improved service delivery and responsiveness” as the most compelling reason to invest in cloud-native or hybrid infrastructure.

The message is clear: IT modernization isn’t just about keeping up — it’s about delivering public value with confidence, transparency, and resilience.

Modernizing public sector IT is complex — but it doesn’t have to be chaotic. Download Anchor Bridge Innovation’s White Paper, *“Meeting Compliance, Security, and Performance Goals with Next-Gen Infrastructure,”* to see how agencies can modernize infrastructure while staying compliant and secure.

About Anchor Bridge Innovations

Anchor Bridge Innovations is a high-tech Value-Added Reseller founded by seasoned IT professionals. We deliver secure, scalable, and future-ready technology solutions tailored to the needs of small and mid-sized enterprises. By partnering with top-tier OEMs and next-gen innovators, we offer a full spectrum of services — including data infrastructure, cloud, cybersecurity, automation, and networking — all backed by white-glove support from planning through post-deployment.

At ABI, we don’t just sell technology — from acquisition to deployment, we speak compliance and delivery.