Cloud Migration for Government

Move to Azure Government to meet federal cybersecurity requirements and reduce the cost of aging on-premises infrastructure.

EXECUTIVE SUMMARY

Your agency carries the operational and financial burden of aging on-premises server infrastructure. Hardware maintenance consumes IT budget that should fund services. Disaster recovery is inconsistent. Remote access for staff creates security exposure. Armely migrates your agency to Microsoft Azure Government, a FedRAMP-authorized cloud environment built for public sector security and compliance requirements.

THE BUSINESS PROBLEM

Government agencies manage IT infrastructure built for a different era. Physical servers require capital investment, facilities space, and constant maintenance. They do not scale during peak service demand. Disaster recovery plans are often outdated or untested. Capital budget cycles make timely hardware replacement difficult even when security requires it. A hardware failure takes public-facing services offline at exactly the moment constituents need them.

HOW ARMELY SOLVES IT

Armely helps your agency **reduce infrastructure cost and meet cybersecurity requirements** by moving your priority systems to **Azure Government**, a FedRAMP-authorized cloud environment built for public sector compliance. Your staff accesses systems securely from any location, disaster recovery becomes reliable and tested, and your IT team redirects capacity from hardware maintenance to service improvement.

BUSINESS OUTCOMES

- Reduce infrastructure costs by **20 to 30%**
- Meet FedRAMP, CJIS, or state cybersecurity framework requirements
- Improve disaster recovery from **days to hours**
- Enable secure remote access for all agency staff
- Eliminate hardware refresh cycles and reduce capital budget pressure

Industry Scenario

Administrative Infrastructure — State Agency

A state agency migrates administrative and reporting infrastructure to Azure Government. Infrastructure costs drop by 25%. During a facilities disruption, staff access systems remotely without service interruption. The next IT audit shows full compliance with state cybersecurity requirements. The IT team redirects 30% of its capacity from maintenance to service improvement.

WHY THIS MATTERS NOW

Federal and state agencies face increasing pressure to close cybersecurity gaps and modernize infrastructure. CISA guidance and state auditors are specifically scrutinizing on-premises environments. Cloud environments provide the security controls, monitoring capabilities, and compliance documentation that auditors now expect. Agencies that delay carry both financial and security risk.

RECOMMENDED NEXT STEP

Schedule a cloud readiness review with your IT director this week. If you want Armely to run that review with you, contact us at info@armely.com or **972-460-0643**. We can turn around a findings report within **5 business days.**

Armely is a certified HUB (Historically Underutilized Business) and Small Business vendor.