

Securing the AI Era in State & Local Government

How Cloudflare and Presidio helps agencies adopt AI safely and defend public services, in plain terms for agency leaders.

Thank you for your interest
in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASPO, TIPS, E&I and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Cloudflare, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.



To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com



Explore More Resources:
carah.io/CloudflareResources



Join Events & Webinars:
carah.io/CloudflareEvents



Discover Technology Solutions:
carah.io/solve



Learn About Procurement:
carah.io/CloudflareContracts



Connect With Our Team:
Cloudflare@carahsoft.com
(703) 230 7577

PUBLIC SECTOR · EXECUTIVE SUMMARY

Securing the AI era in state & local government

How Presidio and Cloudflare help agencies adopt AI safely and defend public services, in plain terms for agency leaders.

THE SHIFT Agency staff are adopting AI faster than policy can keep up, often with constituent data. At the same time, attackers use AI to hit ransomware-prone, under-staffed public systems harder. Both are solved on one platform with FedRAMP High and GovRAMP Authorizations.

1 Safe AI adoption for agency staff

The problem: caseworkers, clerks, and analysts use public AI tools to draft and summarize, sometimes pasting in citizen PII, case files, or benefits data. That is a privacy-law, public-records, and constituent-trust risk, and agencies are also standing up AI to serve residents.

CLOUDFLARE'S ANSWER

- **See it.** Discover which AI tools staff use across every department, including unsanctioned ones.
- **Control it.** Approve tools by department and role; block the rest.
- **Protect constituent data.** Stop PII, case, and benefits data being pasted or uploaded into public AI.
- **Govern resident-facing AI.** AI Gateway gives one place to see, limit, and guardrail the AI services agencies build.

WHY IT'S DIFFERENT

- **Built for government.** A FedRAMP High and GovRAMP Authorized platform you can inherit controls from (NIST SP 800-53, FIPS 140-3), with US data residency, not a stripped-down "gov enclave."
- One platform covers both the AI staff **use** and the AI agencies **build**.

Protect constituent data

Meet privacy & records duties

Adopt AI with guardrails

Modernize within budget

2 Defending public services against AI-accelerated attacks

The problem: government is a top target. Ransomware shuts down courts, 911, and permitting; hacktivists and nation-states hit public sites; AI writes flawless phishing for public employees and probes legacy systems. Benefits, tax, and payment portals face AI-driven fraud, all against lean teams and tight budgets.

CLOUDFLARE'S ANSWER

- **Keep services online.** Absorb denial-of-service attacks and block bots, fraud, and app exploits at network scale, no agency hardware.
- **Protect resident-facing AI.** Screen prompts to citizen chatbots for manipulation and data leaks.
- **Shrink the human target.** Filter malicious email and replace legacy VPN with zero trust, so a stolen password alone does not open the door.

WHY IT'S DIFFERENT

- **Scale absorbs what agency gear cannot.** ~230B threats blocked daily across ~20% of the web means new techniques are caught early.
- One platform replaces overlapping tools, cutting cost and consoles for short-staffed teams.

Stop ransomware entry points

Keep public services online

Protect benefits & payment portals

Do more with a lean team

WHY CLOUDFLARE FOR GOVERNMENT

230B

cyber threats blocked per day (2025 avg)

FedRAMP

High Authorized

GovRAMP

Authorized (fmr. StateRAMP)

337+

cities, 125+ countries

500 Tbps

network capacity to absorb attacks

One platform, not a limited enclave. The same software runs in every Cloudflare data center, so agencies get the full commercial feature set with government-grade controls, inheriting NIST SP 800-53 and FIPS 140-3 with US data residency.

THE SELLER CHEAT SHEET

DISCOVERY QUESTIONS

- Which AI tools are staff using to handle constituent records, and is that list complete?
- If citizen PII landed in a public chatbot, would you know, and could you meet your records and breach duties?
- When did you last test what happens to courts, 911, or permitting if ransomware or DDoS hits?
- Are you putting AI in front of residents? Who secures it, and on what compliance path?

HANDLE THE OBJECTION

"We must stay on a compliant path." Cloudflare for Government is FedRAMP High and GovRAMP Authorized and delivers the full platform, not a stripped-down enclave, inheriting NIST 800-53 and FIPS 140-3.

"No budget or staff for more tools." Consolidating onto one platform usually cuts cost and the number of consoles a lean team has to run.

Opener: "Your staff are using AI on constituent data, and attackers are using AI to hit public services. Let's make both safe, on a platform built for government."

THE PRESIDIO + CLOUDFLARE PLAY

CLOUDFLARE BRINGS THE PLATFORM

A FedRAMP High and GovRAMP Authorized network that governs staff AI use, keeps public services online, and secures the resident-facing AI agencies build.

PRESIDIO BRINGS THE OUTCOME

Public-sector advisory, the assessment that finds the risk, design that fits agency environments, tool consolidation, and **managed services** for lean teams. **Confirm contract vehicles & offers with your Presidio alliance contact.**

Sources: Cloudflare company, network & public-sector materials, Q4 2025 / 2026. Cloudflare for Government holds FedRAMP High and GovRAMP (formerly StateRAMP) Authorizations; see the FedRAMP Marketplace for the current listing. Product capabilities per Cloudflare documentation, June 2026; packaging varies by plan. Items in blue depend on Presidio's Cloudflare agreement and public-sector practice. Non-technical brief; engage your Presidio technical team and Cloudflare for architecture, compliance detail, and a tailored demo.

Page 2 of 2