BeyondTrust | FOR PUBLIC SECTOR

GOVERNMENT SOLUTIONS

Zero Trust PAM

A Mission-Ready Checklist for Government

Zero Trust initiatives across the public sector have reached a decisive point. Strategy is giving way to execution, and privileged access has become one of the most urgent control areas because it sits at the intersection of identity, workload access, and mission uptime. As agencies expand cloud adoption, modernize legacy systems, and support a growing ecosystem of contractors and third parties, the risk associated with standing privileges, exposed remote pathways, and fragmented tooling increases.

This evaluation checklist is designed to help public sector security and IT leaders assess whether a Zero Trust PAM and Privileged Remote Access approach can deliver measurable risk reduction, faster compliance, and operational efficiency without disrupting mission execution. It focuses on the core capabilities agencies should validate during RFI, RFP, and pilot phases, including identity and policy enforcement, session security, credential governance, resilience, integration for audit evidence, and clear pathways for modernization. The goal is to confirm not just feature availability, but real-world readiness to reduce exploitable privilege, improve oversight, and centralize secure access across IT, cloud, and OT environments.

HOW TO USE THIS CHECKLIST

Use the checkboxes for baseline compliance and add a simple score if helpful:

0 Not available
1 Partial or roadmap
2 Available with configuration
3 Mature and proven in production

Also note whether each item is required for ATO, required for pilot exit, or desired enhancement.

Below is a checklist of common security capabilities teams will typically require to establish a strong foundation and successful implementation of Zero Trust PAM. Learn how BeyondTrust privileged access management (PAM) and identity security capabilities address these requirements.

Evaluation Areas	Checklist	Score
Program Fit **Evidence to request** • **Architecture diagrams for GovCloud deployment** • **FedRAMP package details (control inheritance summary, SSP overview)** • **Sample phased deployment plan with timelines**	☐ FedRAMP authorization at the required level and operated in AWS GovCloud, with parity of features available in the authorized environment. ☐ Supports privileged remote access across IT, cloud, and OT within a unified approach, minimizing tool sprawl. ☐ Enables deployment in days with incremental rollout, reducing operational disruption and enabling early risk reduction. ☐ Demonstrates reduced complexity compared to multi-tool stacks through fewer infrastructure components and simplified onboarding. ☐ Provides a clear path to reduce or retire legacy VPN and exposed RDP risk using brokered access approaches.	☐ ☐ ☐ ☐ ☐
Identity and Policy **Evidence to request** • **Sample policy models by persona: admin, operator, contractor** • **Approval workflow examples with audit outputs** • **CAC/PIV test cases and screenshots**	☐ CAC and PIV enforcement, including PIV pass-through into the session where applicable. ☐ Role-based and time-based access policies with structured approvals. ☐ Just-in-time elevation aligned to least privilege for tasks and workflows. ☐ Enforces policy at the point of access, not just at the network perimeter. ☐ Break-glass access with recorded use, bounded scope, and automatic expiry. ☐ Supports secure access for internal users and third parties with governance aligned to agency	☐ ☐ ☐ ☐ ☐ ☐

BeyondTrust | FOR PUBLIC SECTOR

Evaluation Areas	Checklist	Score
Session Security **Evidence to request** • **Sample session recordings and audit logs** • **Demonstration of command filtering and policy enforcement** • **Use cases for HMI, SCADA, PLC access if OT is in scope**	☐ Brokered, encrypted sessions that do not expose targets broadly on the network. ☐ Full monitoring and recording with real-time termination authority. ☐ Command and action controls to reduce risk of unauthorized or high-impact changes. ☐ Strong session governance across Windows, Linux, network devices, cloud consoles, and OT interfaces. ☐ Supports granular oversight required for mission systems and regulated environments.	☐ ☐ ☐ ☐ ☐
Secrets and Credentials **Evidence to request** • **Rotation policy templates** • **Cloud credential entitlements brokering demonstration**	☐ Built-in vault with rotation, checkout governance, and least privilege controls. ☐ Supports ephemeral credentials for cloud consoles and APIs where feasible. ☐ Reduces or eliminates persistent keys and standing access for privileged workflows. ☐ Provides a credible roadmap to remove third-party VPN dependence for privileged access.	☐ ☐ ☐ ☐
Resilience and Scale **Evidence to request** • **Reference architectures for HA** • **Stress testing outcomes** • **Continuity of operations documentation**	☐ Active-active continuity with documented RTO and RPO targets aligned to agency requirements. ☐ High availability across regions and zones as applicable. ☐ Proven scale for contractors, vendors, and multi-agency use, including policy segmentation. ☐ Evidence of performance under peak demand and incident conditions.	☐ ☐ ☐ ☐

BeyondTrust | FOR PUBLIC SECTOR

Evaluation Areas	Checklist	Score
Integrations and Evidence **Evidence to request** • **Sample SIEM dashboards and log mappings** • **Pre-built report inventory** • **Control-to-capability mapping matrix**	☐ ServiceNow integration for request, approval, and ticketbased governance. ☐ Entra ID and other IdPs for identity and policy inheritance. ☐ SIEM for centralized logging and evidence management. ☐ Audit-ready reports aligned to NIST 800-53, CJIS, FIPS and related frameworks. ☐ Out-of-the-box integration expectations are realistic and do not require excessive custom development.	☐ ☐ ☐ ☐ ☐
Migration and Success **Evidence to request** • **Clear implementation plan** • **Pilot success scorecard** • **Free or low-cost training calendar and role-based learning paths**	☐ Clear pathways for first-time PAM, Privileged Remote Access expansion, and legacy modernization. ☐ Built-in scanning or discovery support that reduces time to inventory and onboard systems. ☐ Training for admins, approvers, auditors, and operations teams. ☐ References in regulated public sector environments matching your mission and compliance profile.	☐ ☐ ☐ ☐

RECOMMENDED PILOT EXIT CRITERIA

Security outcomes

- ☐ At least one high-risk privileged workflow moved from legacy remote access to brokered Privileged Remote Access.
- ☐ Just-in-Time (JIT) policies enforced for targeted roles.
- ☐ Session recording and termination validated.

Operational outcomes

- ☐ Approval workflows functioning with ServiceNow or equivalent.
- ☐ Admin overhead reduced versus prior approach.
- ☐ End-user access time improved without policy exceptions.

Compliance outcomes

- ☐ Evidence exported to SIEM.
- ☐ Auditor-ready reporting validated against agency controls.

BeyondTrust | FOR PUBLIC SECTOR

Mission Ready and FedRAMP Authorized: BeyondTrust PAM & Identity Security Solutions

Zero Trust PAM is a mission enabler, not just a security enhancement. Agencies need a path that reduces exploitable privilege, strengthens oversight of internal and third-party access, and delivers rapid time to value without adding complexity. BeyondTrust Privileged Remote Access is designed to unify secure access across IT, OT, and cloud, replace fragmented legacy methods, and provide the visibility and control public sector teams require to meet modern compliance and operational demands.

Next Steps:

Turning Criteria into Measurable Outcomes

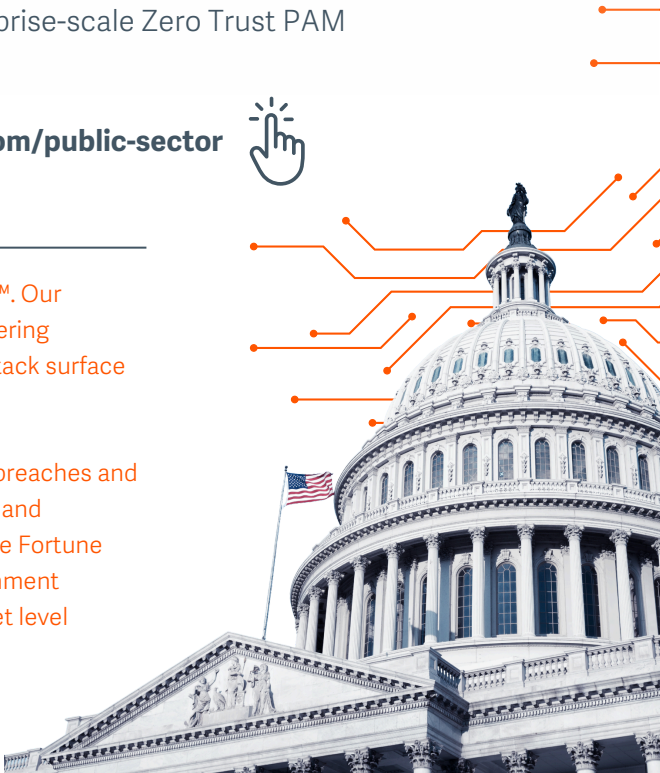
With the evaluation criteria established, the next step is to align stakeholders from security, identity, infrastructure, cloud, OT if applicable, and audit on what "good" looks like for your environment and the compliance outcomes you must prove.

Use this checklist to identify your top three priority use cases and highest-risk access pathways, then scope a focused pilot that validates CAC and PIV enforcement, just-in-time policy, brokered session controls, and evidence export to your SIEM and ticketing workflows.

Define clear pilot exit criteria tied to measurable outcomes such as reduction of standing privileges, elimination of exposed remote access methods for prioritized systems, improved approval and auditability, and demonstrable time-to-value.

Finally, map successful pilot results to a phased production rollout plan that begins with the most critical systems and most frequent privileged workflows, ensuring the program delivers early risk reduction while building a durable foundation for enterprise-scale Zero Trust PAM and Privileged Remote Access adoption.

Contact BeyondTrust today, or learn more here: beyondtrust.com/public-sector



BeyondTrust is the global identity security leader protecting Paths to Privilege™. Our identity-centric approach goes beyond securing privileges and access, empowering organizations with the most effective solution to manage the entire identity attack surface and neutralize threats, whether from external attacks or insiders.

BeyondTrust is leading the charge in transforming identity security to prevent breaches and limit the blast radius of attacks, while creating a superior customer experience and operational efficiencies. We are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.. BeyondTrust has over 2400+ government customers. and our solutions are deployed across all 50 states and in all cabinet level Federal Civilian agencies and over 100 Defense Department environments

Learn more at beyondtrust.com