PUBLIC SAFETY CLOUD STANDARDS (PSCS)

Agency Cloud Readiness Self-Assessment

Version 1.1

Agency Name: ___________________________

Primary Contact: ________________________

Title: _________________________________

Date Submitted: ________________________

1. Purpose of This Assessment

The PSCS Agency Cloud Readiness Assessment is designed to help public safety agencies evaluate their operational, technical, financial, and organizational preparedness for migration to cloud-hosted public safety systems.

This document is intended to be completed by the agency.

Agencies are encouraged to provide:

- Written narrative responses
- Supporting documentation where available
- Honest evaluation of gaps or constraints
- Identification of known risks

Responses will be reviewed and independently scored by PSCS or the designated advisor.

2. Maturity Scoring Model (Agency Self-Assessment)

Agencies should self-assess each section using the following scale:

Score	Maturity Level	Description
0	Not Addressed	No formal process or documentation exists
1	Informal / Reactive	Issues handled as they arise
2	Documented	Processes exist but inconsistently followed
3	Defined & Repeatable	Standardized and consistently followed
4	Measured & Managed	Performance is monitored and reported
5	Optimized	Continuous improvement and proactive management

Agencies should retain documentation supporting each score.

3. Governance & Leadership

Objective

Determine whether executive and operational leadership are aligned and capable of sponsoring a cloud transition.

Please describe:

- Executive sponsorship for cloud evaluation
- Defined strategic goals (resilience, staffing relief, cost stability, etc.)
- Documented IT governance structure
- Assigned cybersecurity ownership
- Board/city/county approval requirements
- Current IT roadmap

Attachments (if available):

☐ Strategic IT plan

☐ Organizational chart

☐ Governance documentation

☐ Security ownership documentation

Agency Response:

Self-Score (0–5): _______

4. Staffing & Operational Capacity

Objective

Assess internal capacity to maintain on-prem systems or transition to cloud services.

A. Staffing Capacity

Describe:

- Current IT staffing levels
- Average weekly overtime
- Single points of failure (critical knowledge concentration)
- 24/7 coverage capability
- Succession planning efforts

Attachments (if available):

☐ Staffing roster

☐ Coverage schedule

☐ Workload documentation

Agency Response:

Self-Score (0–5): _______

B. Networking Skills

Describe staff experience with:

- VLAN segmentation
- Firewall and VPN configuration
- Redundant ISP configuration
- Maintenance of network diagrams

Attachments (if available):

☐ Network diagrams

☐ Configuration documentation

Agency Response:

Self-Score (0–5): _______

C. Security Expertise

Describe:

- Dedicated security personnel (if any)
- CJIS compliance familiarity

- Endpoint Detection & Response deployment
- Incident response planning and testing

Attachments (if available):

☐ Security policies

☐ Incident response documentation

Agency Response:

Self-Score (0–5): _______

D. Infrastructure Operations

Describe:

- Patch management cadence
- Server lifecycle planning
- Hardware procurement planning
- Centralized monitoring tools in place

Attachments (if available):

☐ Patch reports

☐ Asset inventory

☐ Monitoring dashboards

Agency Response:

Self-Score (0–5): _______

5. Network & Hardware Infrastructure

Objective

Evaluate infrastructure readiness for hybrid or full cloud deployment.

A. ISP & Redundancy

Describe:

- Number of ISPs
- Automatic failover configuration
- Most recent outage (date & duration)
- ISP SLAs

Attachments (if available):

☐ ISP contracts

☐ Failover configuration documentation

Agency Response:

Self-Score (0–5): _______

B. LAN/WAN Architecture

Describe:

- Current network diagram availability
- Age of core switches
- QoS configuration for dispatch systems

- Network segmentation practices

Agency Response:

Self-Score (0–5): _______

C. Firewall & Edge Security

Describe:

- Firewall make/model
- Firmware currency
- VPN throughput adequacy
- Encryption standards supported
- IDS/IPS usage

Agency Response:

Self-Score (0–5): _______

D. Hardware Lifecycle

Describe:

- Average server age
- Storage redundancy model
- Hardware refresh cycle
- Warranty/support coverage

Agency Response:

Self-Score (0–5): _______

6. Software Evaluation & Vendor Strategy

Objective

Assess preparedness to evaluate and transition software vendors.

A. Evaluation Process

Describe:

- Whether vendors are currently being evaluated
- RFP process structure
- Inclusion of uptime/security in scoring
- Security documentation review process

Agency Response:

Self-Score (0–5): _______

B. Vendor Comparison & Cost Modeling

Describe:

- Cloud vs on-prem comparison methodology
- Total Cost of Ownership calculation
- SLA review process
- Exit strategy considerations

Agency Response:

Self-Score (0–5): _______

C. Existing Vendor Transition

Describe:

- Current vendor’s cloud offering
- Migration path clarity
- Data ownership understanding
- Integration impact assessment

Agency Response:

Self-Score (0–5): _______

7. On-Premise Operational Maturity

Objective

Determine sustainability of maintaining on-prem infrastructure.

A. Endpoint Security

B. Active Directory & DNS

C. Monitoring & Alerting

D. Backup & Recovery

E. Patch & Vulnerability Management

For each area, describe current controls, documentation, and testing practices.

Agency Response:

Self-Score (0–5): _______

8. Business Continuity & Disaster Recovery

Describe:

- Defined RTO and RPO
- Secondary dispatch location
- Generator/UPS backup
- Frequency of DR testing
- Most recent DR exercise date

Attachments (if available):

☐ DR plan

☐ Test documentation

Agency Response:

Self-Score (0–5): _______

9. Financial Readiness & Cost Awareness

Describe:

- 5-year hardware refresh forecast
- Power and cooling cost visibility
- Staff burden cost estimates
- Overtime impact
- Budget constraints (capital vs operational)

Attachments (if available):

☐ Budget documentation

☐ Capital planning documents

Agency Response:

Self-Score (0–5): _______

10. Data & Integration Complexity

Describe:

- Number of CAD integrations
- RMS integrations
- Jail integrations
- Body camera integrations

- State/NLETS connectivity
- GIS complexity
- API dependencies

Attachments (if available):

☐ Integration list

☐ Interface agreements

Agency Response:

Self-Score (0–5): _______

11. Change Management & Organizational Readiness

Describe:

- Prior IT transitions
- Anticipated user resistance
- Training budget allocation
- Communication plan

Attachments (if available):

☐ Project documentation

☐ Training plans

Agency Response:

Self-Score (0–5): _______

12. Agency Attestation

I certify that this assessment reflects our current operational capabilities and known constraints.

Name: ___________________________

Title: ___________________________

Signature: _______________________

Date: ___________________________

13. Overall Readiness Determination (To Be Completed After Review)

☐ Ready for Cloud Migration

☐ Hybrid Approach Recommended

☐ On-Prem Hardening Required Before Migration