PUBLIC SAFETY TECH

Guide to Creating a Public Safety Technology RFP

A strong RFP defines operational outcomes, security expectations and realistic workflows without copying one vendor's feature list or prescribing unnecessary design details.

14 MIN READ | AUGUST 2026

IN SHORT

A practical guide to writing outcome-focused public safety technology RFPs, evaluating vendors and conducting demonstrations based on real workflows.

A public safety technology RFP should help an agency select the best solution, not reward the vendor that checks the most boxes.

A well-designed request for proposals creates a fair process, gives vendors enough information to respond accurately and helps evaluators compare more than marketing claims. A poorly designed RFP can lock the agency into outdated assumptions, discourage strong vendors and produce responses that are difficult to compare.

The RFP should translate an operational need into a structured buying process. It should explain what the agency is trying to improve, establish minimum responsibilities and give vendors room to demonstrate how they would solve the problem.

Before beginning, confirm whether an RFP is required. A request for information, cooperative contract, competitive quotation, pilot or other procurement method may better fit the scope and local rules. Work with procurement and legal staff early.

Define the Problem and Outcome

Do not begin with a feature list. Begin with the problem.

Describe:

- The current workflow
- The people who perform it
- The information and systems involved
- Delays, errors, duplicate entry and workarounds
- Operational or compliance consequences
- The result leadership expects to improve

For example, “The agency needs scheduling software” is too broad. A stronger explanation may state that officers spend several hours filling open positions, members cannot see real-time availability, qualification rules are checked manually and leadership lacks warning when staffing falls below minimum levels.

Define measurable outcomes such as reduced administrative time, improved certification compliance, faster applicant follow-up, fewer unfilled shifts or quicker report preparation.

Separate four levels of need:

1. **Mandatory:** The solution cannot meet the agency's need without it.
2. **Highly desirable:** Creates meaningful value but may have an acceptable alternative.

3. **Optional:** Worth considering if provided without undermining priorities.

4. **Future:** Not required now, but relevant to roadmap and scalability.

Too many mandatory requirements eliminate useful competition. Use “must” only when the agency is prepared to reject a solution that cannot satisfy it.

Research Before Writing

Agencies should understand the market before publishing requirements.

Talk with peer agencies, professional associations, IT leaders and subject-matter experts. Review available products and common implementation models. A non-binding request for information can help clarify terminology, integration approaches, typical pricing and realistic timelines.

Market research should inform the RFP without turning it into one vendor's specification. Avoid copying product pages or another agency's RFP without confirming that the requirements match your workflow.

Document vendor conversations according to procurement rules. Once a formal process begins, provide equal access to clarifications and avoid private guidance that creates an unfair advantage.

Build the Right Team

Create a small core team with enough authority and knowledge to move the process forward.

Potential participants include:

- Executive sponsor
- Operational users

- System administrators
- IT and cybersecurity
- Records, privacy or compliance staff
- Procurement
- Finance
- Legal counsel
- Training and implementation leaders
- Accessibility or human-resources representatives

Assign one project owner. That person coordinates decisions, schedules, questions, documents and communication with vendors.

Define roles before evaluation:

- **Q** Who approves the final RFP?
- **Q** Who answers vendor questions?
- **Q** Who determines whether a requirement is mandatory?
- **Q** Who scores written proposals?
- **Q** Who attends demonstrations?
- **Q** Who may participate in pricing or contract negotiations?
- **Q** Who makes the final recommendation?

Include ordinary users, not only leadership. Administrators and frontline personnel often identify workflow problems that are invisible in executive summaries.

Require evaluators to disclose conflicts and protect vendor information according to law and policy.

Provide Agency Context

Vendors cannot propose accurate pricing, architecture or implementation without understanding the agency.

Provide relevant information such as:

- Agency type and jurisdiction
- Career, volunteer or combination structure
- Number of members, employees and administrators
- Stations, companies, divisions or locations
- Expected users and permission groups
- Approximate data and attachment volume
- Current software and contract dates
- Required integrations
- Devices, browsers and network constraints
- Single sign-on or identity requirements
- Accessibility expectations
- Records-retention and security policies
- Desired launch date and known deadlines
- Available internal project resources

Identify information that cannot be shared publicly and provide a controlled method for qualified vendors to receive it when appropriate.

Explain current pain points without exposing sensitive vulnerabilities. Vendors need enough context to propose a solution, not a roadmap for attacking the agency.

Create a Clear RFP Structure

A practical technology RFP usually includes:

1. Notice and procurement schedule
2. Agency background

3. Project purpose and desired outcomes
4. Current environment
5. Scope of work
6. Functional and workflow requirements
7. Technical and integration requirements
8. Security, privacy and continuity requirements
9. Data migration and ownership
10. Implementation and training
11. Support and service levels
12. Vendor qualifications and references
13. Pricing format
14. Proposal instructions
15. Evaluation process
16. Contract terms and required forms

Use consistent numbering so vendors can respond directly to each requirement. Provide required response tables or workbooks when they improve comparison, but allow narrative explanation where context matters.

State page limits, file formats, deadlines, question procedures and required signatures clearly. Administrative ambiguity can disqualify an otherwise strong response.

Write Requirements Around Workflows

Requirements should describe the result and operating context.

Instead of writing, “The system must include a dashboard,” explain what the user must see, which decisions the information supports, how frequently it updates and which permissions apply.

Use workflow scenarios such as:

- A member uploads a renewed certification that requires officer approval.
- A scheduler fills an open position that requires a specific rank and qualification.
- An administrator changes a member's station and role with a future effective date.
- A supervisor sends a critical policy update and confirms acknowledgment.
- A system integration stops updating during a weekend.
- The agency requests a complete export before contract renewal.

Ask vendors to identify whether each capability is:

- Available in the current standard product
- Available through configuration
- Requires custom development
- Provided by a partner
- Planned for a future release
- Not available

Require explanations for partial compliance. A simple yes or no can hide important limitations.

Avoid requirements copied from one vendor's terminology unless the exact capability is essential.

Define Technical and Integration Requirements

Describe the agency's technology environment and required connections.

For each integration, identify:

- Source and destination systems
- Information exchanged
- Direction of data flow
- Update frequency
- Expected volume
- API, file or other available method
- Authentication requirements
- Vendor contacts and costs
- Error handling and monitoring
- Which party supports the connection

Do not accept “integrates with” as a complete answer. Ask vendors to describe what works today and to demonstrate it when possible.

Request supported browsers, devices, mobile capabilities, accessibility, identity management, hosting architecture, data locations and expected agency network changes.

Avoid prescribing a specific cloud provider or development language unless a legitimate requirement makes it necessary. Focus on security, compatibility, support and outcomes.

Include Security and Continuity

Create a security section proportionate to the data and operational risk.

Request clear responses about:

- Data ownership and permitted use
- Hosting and data location
- Encryption in transit and at rest
- Multifactor authentication and single sign-on
- Role and field-level permissions
- Vendor-employee access
- Audit logs
- Secure development and vulnerability management
- Independent assessments and their scope
- Monitoring and incident response
- Breach-notification timing
- Backups and restoration testing
- Uptime history and service commitments
- Disaster recovery
- Cyber insurance
- Subprocessors and AI services
- Complete data export
- Retention and deletion
- Continuity if key personnel or the company become unavailable

Use a separate security questionnaire when detail would overwhelm the main RFP. Make it part of the evaluation and final agreement, not an exercise collected and forgotten.

State whether security exceptions are disqualifying, scored or subject to remediation before launch.

Address Data Migration and Exit Before Purchase

Describe the current data sources, approximate volumes, quality concerns, attachments and required history.

Ask the vendor to explain:

- Data templates and supported formats
- Cleanup and transformation responsibilities
- Historical backfill limits
- Test migrations
- Validation and acceptance
- Handling of duplicates and failed records
- Attachment migration
- Migration schedule and fees

Also define exit requirements. The agency should be able to export usable records, attachments, history and audit information throughout the contract and at termination.

A responsible procurement process plans both entry and exit.

Define Implementation Expectations

Require a proposed implementation approach that includes:

- Vendor and agency project roles
- Discovery and workflow confirmation
- Configuration decisions
- Data migration
- Integration setup
- Security review
- Testing and acceptance
- Administrator training
- Role-based user training
- Communication and launch support
- Post-launch review

Ask for a realistic schedule with dependencies. Require vendors to identify assumptions such as agency response time, data quality, third-party cooperation and available staff.

Define acceptance. Go-live alone should not prove success. Acceptance may require completed migration, functioning integrations, documented training, resolved critical defects and agreed test results.

Request a 30-, 60- or 90-day review after launch to address adoption, unresolved issues and configuration improvements.

Define Support and Service Levels

Ask how users and administrators receive help, which hours are covered and how urgent issues are escalated.

Request:

- Support channels
- Standard and emergency hours
- Severity definitions
- Response and restoration targets
- Escalation process
- Status communications
- Planned-maintenance notice
- Named account or success resources
- Included training and documentation
- Costs for premium support

Distinguish response time from resolution time. An automated acknowledgment within five minutes does not mean the problem is being worked.

Ask who owns support when a problem involves an integration partner. The agency should not be left coordinating two vendors that each blame the other.

Create a Weighted Scoring Model

Build the scoring model before proposals arrive.

A sample weighting might be:

CATEGORY	EXAMPLE WEIGHT
Operational and functional fit	30%
Usability and accessibility	10%

CATEGORY	EXAMPLE WEIGHT
Security, privacy and continuity	15%
Implementation and migration	10%
Support and vendor capability	10%
Demonstration and workflow validation	15%
Total cost	10%

Adjust weights to the project. A mission-dependent system may place greater weight on security and reliability. A widely used member application may increase usability and accessibility.

Define scoring anchors. Explain what qualifies as excellent, acceptable, weak or noncompliant. This improves consistency across evaluators.

Separate mandatory pass-or-fail items from scored preferences. Document consensus meetings and changes according to procurement policy.

Price should matter, but the lowest initial price may create higher migration, support or long-term costs.

Require Comparable Pricing

Provide a pricing template that captures the complete cost.

Request:

- Implementation and project management
- Data migration and cleanup
- Configuration and customization
- Integrations
- Subscription or licensing
- User, location, storage or usage charges
- Training

- Support levels
- Hardware or devices
- Travel
- Optional modules
- Renewal increases or pricing formula
- Future expansion
- Export or termination assistance

Ask for pricing across several years and require vendors to state assumptions. Identify which charges are one-time, recurring, estimated or dependent on third parties.

Avoid comparing one vendor's base package with another vendor's complete implementation.

Control Demonstrations

Do not let demonstrations become unrestricted sales presentations.

Provide finalists with the same scenarios, users, data conditions and time limits. Reserve a portion for vendor-selected differentiators, but require the agency workflows first.

Example demonstration script:

1. Complete a routine user task from a phone.
2. Show an administrator configuring the workflow.
3. Demonstrate permissions for two different roles.

4. Handle missing or incorrect information.
5. Show reporting and export.
6. Demonstrate an integration and its error status.
7. Show the support path when something fails.

Use current production functionality. Clearly label prototypes, partner products and roadmap items.

Allow evaluators to record scores individually before group discussion. Capture unanswered questions and require written follow-up by the same deadline for all finalists.

Consider a sandbox or pilot for high-risk decisions, with defined success criteria and data protections.

Check References and Contracts

Request references from agencies with similar size, structure, integrations and use cases. Do not rely only on the vendor's largest or happiest customer.

Ask references:

- **Q** What took longer than expected?
- **Q** What required more agency effort?
- **Q** Which capability did not work as demonstrated?
- **Q** How does support respond during serious problems?
- **Q** Have integrations remained reliable?

- **Q** Has pricing remained predictable?
- **Q** How has the product changed?
- **Q** Would the agency select the vendor again?

Search for public status information, contract records, major incidents and customer experiences where appropriate.

The final contract must match the winning proposal and negotiated commitments. Review data ownership, security, service levels, pricing, renewals, insurance, implementation, acceptance, termination, export and transition assistance.

Do not assume an RFP response automatically becomes contractually binding. Incorporate the relevant proposal, security response and clarifications by reference or attachment.

Manage Vendor Questions and Amendments

Set a formal period for questions. Publish answers to all participating vendors without identifying who asked unless required.

When a question reveals ambiguity or an unrealistic requirement, issue an amendment. Give vendors adequate time to adjust responses.

Maintain one authoritative RFP package containing the original document and every amendment. Require vendors to acknowledge all amendments.

Document the Decision

Maintain evaluation records, scores, notes, clarifications, conflict disclosures and approvals according to procurement and public-record requirements.

The final recommendation should explain why the selected solution best meets the agency's outcomes, not merely list the final score.

Notify unsuccessful vendors professionally and provide debriefing when permitted. Constructive feedback improves future competition and reduces confusion.

Reusable Public Safety Technology RFP Outline

Use this baseline when planning the document:

- Project title and procurement contact
- Submission deadline and schedule
- Agency background
- Problem statement
- Desired outcomes and success measures
- Current environment and data
- Scope of work
- User and administrator workflows
- Functional requirements
- Technical requirements
- Integrations
- Security, privacy and continuity
- Data migration and ownership
- Implementation and acceptance
- Training
- Support and service levels
- Vendor qualifications
- References
- Pricing workbook
- Demonstration requirements
- Evaluation criteria
- Contract terms
- Required forms and certifications

The outline should be customized. A short, focused RFP is better than a large document filled with requirements the agency will never evaluate.

Final RFP Quality Check

Before release, confirm:

- The operational problem is clear.
- Success measures are defined.
- Mandatory and preferred needs are separated.
- Agency context is sufficient for accurate responses.
- Requirements describe outcomes and workflows.
- Integrations identify real data exchanges.
- Security and ownership questions reflect the data risk.
- Migration, implementation and exit are addressed.
- Pricing can be compared across vendors.
- Demonstration scenarios are ready.
- Scoring weights and anchors are approved.
- Procurement, legal, IT and operational stakeholders completed review.
- Dates allow vendors enough time to ask questions and prepare thoughtful responses.

Frequently asked questions

How detailed should a technology RFP be?

Provide enough operational context and required outcomes for comparable responses, but avoid prescribing every interface detail.

Should an RFP include desired features?

Yes, but distinguish required outcomes, preferred features and optional ideas. This protects priorities without eliminating useful alternatives.

How should demonstrations be scored?

Use common workflow scenarios, predefined criteria and evaluators representing both users and administrators.

Should security requirements be included?

Yes. Address hosting, encryption, access, backups, monitoring, incidents, recovery, data ownership and continuity.

What costs should agencies compare?

Compare implementation, migration, licenses, integrations, support, training, increases, hardware and exit or export costs over several years.

For the decision-making philosophy behind this process, read Stop Buying Features. Start Solving Department Problems..

Last reviewed August 2026

Dave Iannone

FOUNDER & CHIEF PRODUCT OFFICER, FIRST ARRIVING

He co-founded Firehouse.com and now leads First Arriving, a public safety SaaS company. A fire service veteran and former journalist, he writes on technology, marketing, recruitment and leadership in and around public safety.

DaveIannone.com | LinkedIn | Contact | Schedule a Meeting