REDLEIF

Evaluation Checklist:

Enterprise Physical Security Platform

A practical, RFX-aligned guide for evaluating integrated physical security platforms

Pre-RFX Supplement | 2026

✓ How To Use This Checklist

This checklist helps you run structured market research and vendor evaluation without writing a full, formal RFX. It delivers many of the same decision-support inputs procurement teams typically build during RFX intake: clear requirements, evidence requests, evaluation criteria, and a documented decision trail.

If you later choose to run a formal RFX, you can use the outputs from this checklist as a plug-in for your requirements attachment, vendor demo script, and scoring rubric.

Step 1. **Start with outcomes and constraints.** Capture mission outcomes, risk boundaries, and required timelines before comparing features.

Step 2. **Run a structured vendor screen.** Share this checklist in advance and ask vendors to respond in writing (short, direct answers).

Step 3. **Hold at least one focused screening call per vendor (we recommend about 60 minutes).** Use the "Minimum bar" items in each section to eliminate poor fits early. If needed, schedule a second deep-dive session for the short list.

Step 4. **Require proof for the requirements that matter most.** For high-risk or complex requirements, ask for a demo, architecture evidence, or a reference that confirms the claim. Use judgment on lower-impact items.

Step 5. **Score what matters.** Weight governance, security, and implementation realities more heavily than "nice to have" capabilities.

Step 6. **Translate into procurement language.** Use the "Evidence to request" lines to build an RFX addendum or requirements attachment.

Success outcome: You can explain, in plain language, why the selected platform is the best value and/or lowest-risk way to deliver unified physical security and emergency response across your facilities, within your timeline and budget constraints.

1. Public Sector Readiness

Security & Compliance Framework

- [ ] Platform demonstrates pathway to FedRAMP, GovRAMP, or equivalent authorization, or already holds relevant certifications
- [ ] Provides encryption at rest and in transit with clear data management and residency controls
- [ ] Supports hybrid or on-premises deployment options where required by policy or connectivity constraints
- [ ] Can articulate how it handles public records retention, FOIA requests, and chain of custody requirements
- [ ] Demonstrates compliance with applicable standards (NDAA Section 889, TAA, accessibility requirements)

Procurement Access

- [ ] Available through GSA Schedule, NASPO, state cooperative contracts, or other relevant vehicles
- [ ] Can provide contract numbers, NAICS codes, and ordering instructions
- [ ] Has successfully completed public sector procurements before (federal, state, or local)

Client Base

- [ ] Provides references from federal, state, or local agencies with similar operational scope
- [ ] Can also point to private sector deployments that demonstrate speed-to-value and operational maturity in similar environments
- [ ] Can name proven use cases that map to your environment. Same-vertical examples are a strong signal, but results from other verticals can often still validate fit for your needs.
- [ ] References include organizations with comparable facility count, geographic distribution, and compliance requirements

Evidence to Request

- Compliance documentation and authorization status
- Sample contract language and procurement vehicle details
- At least three references from public sector clients with contact information

Red Flags

- Vague claims about "government-ready" without specific compliance certifications or authorizations
- Cannot explain data sovereignty, retention policies, or public records handling
- No experience navigating appropriations cycles, multi-year budgets, or oversight requirements

2. Platform Architecture & Integration

Architecture & Infrastructure Requirements

- [ ] Explains clearly what components are cloud-managed versus what runs on local infrastructure
- [ ] Provides transparent view of on-premises infrastructure requirements (servers, storage, management appliances)
- [ ] Can operate effectively in environments with limited or intermittent connectivity (remote facilities, disaster scenarios)
- [ ] Provides clear uptime SLAs and explains redundancy approach
- [ ] Clarifies whether platform is purpose-built as unified system or assembled from acquired point solutions, and can explain what that means for integration depth, update cadence, and long-term roadmap coherence

System Integration & Coordination

- [ ] All security functions (video surveillance, access control, environmental monitoring, visitor management, alarms, intercoms) can be managed through coordinated interfaces
- [ ] Demonstrates how different security systems work together during normal operations and emergencies
- [ ] Badge activity can be correlated with video footage efficiently
- [ ] Environmental alerts (air quality, temperature, humidity) can be viewed alongside cameras and access logs
- [ ] Emergency response actions (lockdowns, unlocking for evacuation) can coordinate across multiple systems

Integration with Existing Infrastructure

- [ ] Can work with existing cameras, access control hardware, or other security investments
- [ ] Explains integration approach: native support, middleware/gateway technology, or requires replacement
- [ ] Provides clear migration path that allows phased deployment without full rip-and-replace
- [ ] Integrates with existing IT systems (Active Directory, SSO, SIEM, incident management platforms)

Evidence to Request

- Architecture diagram showing cloud versus on-site components and data flows
- Demo showing unified response: badge swipe automatically pulling up video, emergency lockdown coordinating doors and cameras
- Documentation on integration capabilities with third-party systems
- Explanation of what happens during network outages (what continues to function, what is degraded)

Red Flags

- Different security systems require separate logins and cannot coordinate during emergencies
- Significant on-premises infrastructure without clear operational support model
- Manual processes required to correlate video, access, and incident data
- Integration requires extensive custom development or ongoing professional services

3. Emergency Response & Operational Speed

Speed of Emergency Response

- [ ] Can demonstrate rapid facility-wide lockdown from mobile device (ask for specific timeframe)
- [ ] Shows how live video can be shared with first responders during active incidents
- [ ] Provides panic button integration with automatic video capture and notification
- [ ] Demonstrates remote unlocking for emergency egress or law enforcement access
- [ ] Mobile apps provide emergency response capabilities, not just viewing

Coordinated Multi-System Response

- [ ] Single action can trigger coordinated response across cameras, doors, alarms, and intercoms
- [ ] Platform automatically captures relevant video, access logs, and environmental data during incidents
- [ ] Demonstrates how security staff can manage multiple facilities simultaneously during emergencies
- [ ] Shows how access permissions and video streams can be granted temporarily to first responders

Operational Complexity

- [ ] Security staff can execute emergency procedures without IT support or complex workflows
- [ ] Interface is intuitive enough that staff can perform critical functions under pressure
- [ ] Training requirements are measured in hours or days, not weeks
- [ ] Can show examples of non-technical staff (facilities managers, school principals, clinic administrators) using the platform effectively

Evidence to Request

- Live demo of emergency lockdown scenario showing coordination across systems and mobile access
- Walkthrough of typical workflows: responding to alarm, investigating after-hours activity, compiling incident report
- Documentation of training requirements and time-to-proficiency for typical users

Red Flags

- Emergency procedures require multiple logins, systems, or complex workflows
- Mobile apps have significantly limited functionality compared to desktop interfaces
- Vendor cannot provide concrete examples of emergency response time from real deployments
- System requires IT staff involvement to perform time-sensitive emergency actions

4. Distributed Operations & Scalability

Multi-Site Management

- [ ] Single dashboard provides visibility across all facilities regardless of geographic distribution
- [ ] Can demonstrate managing 50+ facilities from one interface with clear filtering and search
- [ ] Adding new facilities does not require proportional increase in IT staff or infrastructure
- [ ] Regional offices can be managed centrally or with delegated authority as needed

Remote & Low-Connectivity Locations

- [ ] Supports facilities with limited internet connectivity (parks, remote offices, field locations)
- [ ] Provides cellular/LTE connectivity options where wired networks are impractical
- [ ] Cellular failover is built into devices rather than requiring separate infrastructure
- [ ] Explains what functionality is available during network disruptions
- [ ] Can support solar-powered or battery-backed deployments for remote locations

Operational Efficiency at Scale

- [ ] Demonstrates how one security operator can monitor multiple facilities simultaneously
- [ ] Shows intelligent alerting that filters noise and surfaces actionable events
- [ ] Provides search and investigation tools that work across all cameras and facilities
- [ ] Explains how the platform reduces "swivel chair" operations (switching between multiple systems)

Evidence to Request

- Demo showing multi-site dashboard with realistic facility count
- Case study from organization managing distributed operations (parks, regional offices, multiple campuses)
- Documentation of remote site deployment options and connectivity requirements

Red Flags

- Each facility requires dedicated server infrastructure or on-site IT resources
- Multi-site visibility requires separate logins or manual switching between facility dashboards
- Cannot demonstrate efficient operations for distributed environments
- Adding facilities requires complex configuration or professional services engagement

5. Investigation, Search & Intelligence

Video Search & Analytics

- [ ] Supports intelligent search across all video (search by object, person, vehicle, activity)
- [ ] Provides motion-based search to quickly identify when activity occurred
- [ ] Demonstrates person of interest tracking and alerts across multiple cameras and facilities
- [ ] Can search by vehicle description or license plate number across all locations

License Plate Recognition

- [ ] Built-in license plate recognition without additional hardware, software licensing, or specialized cameras
- [ ] Supports watchlists for stolen vehicles, amber alerts, or persons of interest
- [ ] Can demonstrate alerts when watched vehicles enter or exit facilities
- [ ] Provides audit trail and chain of custody suitable for law enforcement collaboration

Evidence Compilation & Chain of Custody

- [ ] Incident reports automatically compile video, access logs, timestamps, and environmental data
- [ ] Provides timestamped audit trail of all system access and actions taken
- [ ] Supports evidence export in formats suitable for legal proceedings
- [ ] Can demonstrate how video and data are protected from tampering or unauthorized access

Evidence to Request

- Demo of search capabilities: finding specific vehicle, person, or activity across multiple cameras
- Walkthrough of incident report generation showing automatic compilation of relevant data
- Documentation of chain of custody and audit trail capabilities

Red Flags

- Search requires manually reviewing footage or scrubbing through timelines
- Video and access data are in separate systems requiring manual correlation
- Cannot provide tamper-evident audit trails or evidence suitable for legal proceedings
- License plate recognition requires expensive add-on hardware or separate platform

6. Deployment, Implementation & Maintenance

Speed to Deployment

- [ ] First facility can be operational in 30-60 days
- [ ] Clear phased rollout plan starting with pilot facility, then strategic expansion
- [ ] Installation requirements and dependencies are documented upfront (network, power, mounting)
- [ ] Expansion to additional facilities after pilot is low-friction and repeatable

Infrastructure Requirements

- [ ] Clear documentation of network bandwidth, power, and mounting requirements
- [ ] Explains on-premises infrastructure footprint and associated operational burden (servers, storage, backup, updates)
- [ ] Works with existing network infrastructure or explains what network architecture is required
- [ ] Can accommodate facilities with varying levels of IT maturity and infrastructure

IT Operational Burden

- [ ] Does not require dedicated IT staff for security operations
- [ ] Integrates with existing IT management tools (monitoring, alerting, authentication)
- [ ] Provides clear support model and escalation path
- [ ] Demonstrates that security staff can handle day-to-day operations without constant IT support

Ongoing Maintenance, Updates & Hardware Lifecycle

- [ ] Software updates deploy automatically without requiring maintenance windows or IT intervention
- [ ] Can articulate their hardware lifecycle philosophy: how long devices remain supported, whether software updates meaningfully extend device capability after installation, and what the expected replacement cycle looks like
- [ ] Explains what ongoing maintenance is required versus what is handled automatically
- [ ] Hardware has clear warranty and replacement process
- [ ] Can demonstrate how features and capabilities improve over time through updates

Evidence to Request

- Sample implementation timeline with milestones for pilot and expansion phases
- Documentation of infrastructure and network requirements
- Explanation of ongoing maintenance responsibilities (vendor versus customer)
- Case study showing how platform scaled from pilot to full deployment
- Reference contact information for IT operations staff (not just security leadership) who can discuss day-to-day operational requirements
- Clear explanation of hardware support windows and what "end of support" means in practice for deployed devices

Red Flags

- Implementation timeline for initial pilot extends beyond 90 days without clear justification
- Routine operation requires specialized IT staff or ongoing professional services dependency
- Software updates require scheduled downtime or create compatibility risks between components
- Expanding to new facilities requires significant reconfiguration rather than repeatable deployment
- Hardware lifecycle is defined primarily by replacement cycles rather than ongoing capability development

7. User Experience & Adoption

Interface Simplicity

- [ ] Security staff can perform common tasks with minimal training
- [ ] Mobile apps provide intuitive access to critical functions
- [ ] Demonstrates that non-technical facilities or program staff can use visitor management, access control, and basic monitoring
- [ ] Interface design reduces cognitive load during high-stress situations

Mobile-First Operations

- [ ] Full security functionality available from mobile devices, not just viewing
- [ ] Can grant temporary access, respond to alarms, and pull up video from phone
- [ ] Mobile apps work reliably in field conditions (low connectivity, outdoor environments)
- [ ] Push notifications for critical events work consistently

Adoption & Training

- [ ] Training requirements are realistic for typical staff (security officers, facilities managers)
- [ ] Provides documentation, training materials, and ongoing enablement resources
- [ ] Can demonstrate that organizations achieve high adoption rates (70%+ of intended users actively using platform)
- [ ] Shows measurable productivity improvements (time saved on investigations, incident response, routine monitoring)

Evidence to Request

- Hands-on demo where evaluator performs common tasks (pull up camera, lock door remotely, search for vehicle, compile incident report)
- Mobile app demonstration in realistic scenarios
- Reference interviews asking about adoption challenges and training requirements

Red Flags

- Interface requires extensive training or reference documentation for common tasks
- Mobile apps have significantly reduced functionality compared to desktop
- References report low adoption or staff reverting to old systems
- Vendor cannot articulate how platform reduces operational burden versus legacy systems

8. Governance, Audit & Compliance

Audit Trail & Documentation

- [ ] Complete logs of all system access, configuration changes, and security events
- [ ] Automatic linkage of video footage to access events, alarms, and environmental alerts
- [ ] Audit logs suitable for oversight reviews, internal investigations, and legal proceedings
- [ ] Demonstrates data retention policies that align with records management requirements

Privacy & Access Controls

- [ ] Role-based access controls limit who can view cameras, unlock doors, or access sensitive areas
- [ ] Demonstrates how access is granted, monitored, and revoked
- [ ] Can explain privacy controls (redaction, restricted viewing, time-based access)
- [ ] Provides audit visibility into who viewed what footage and when

Retention & Records Management

- [ ] Configurable retention policies by facility, camera, or classification
- [ ] Can accommodate varying retention requirements (30 days standard, 7 years for critical incidents)
- [ ] Explains storage economics and how retention scales
- [ ] Supports legal hold and eDiscovery workflows where applicable

Evidence to Request

- Sample audit log export showing system access, video viewing, and configuration changes
- Demonstration of role-based access controls and privacy features
- Documentation of retention capabilities and storage architecture

Red Flags

- Incomplete audit trails (video separate from access logs, no record of who viewed what)
- Cannot accommodate varying retention requirements across facilities or camera types
- Privacy controls are manual or require custom development
- Audit logs are not tamper-evident or suitable for legal proceedings

9. Cost & Total Cost of Ownership

Pricing Transparency

- [ ] Clear per-device or per-facility pricing model
- [ ] Explains licensing model (per-device vs. per-user vs. per-feature) and how costs scale as organization grows
- [ ] Explains what is included in base price versus optional add-ons
- [ ] Can work within annual budget appropriations and multi-year planning cycles
- [ ] Provides flexible contract terms (annual, multi-year, enterprise agreements)

Total Cost of Ownership

- [ ] Accounts for hardware, software, installation, support, and ongoing maintenance
- [ ] Explains infrastructure costs (servers, network upgrades, storage)
- [ ] Demonstrates cost savings from unified platform (reduced IT burden, staff efficiency, faster investigations)
- [ ] Can quantify operational savings (staff time, maintenance contracts, avoided costs)

When evaluating TCO, consider operational costs that may not be itemized in vendor proposals:

- IT staff time for software updates, security patches, and system maintenance
- Infrastructure refresh cycles (servers, storage, backup systems)
- Disaster recovery infrastructure and routine testing requirements
- Scaling costs: Does adding facilities require proportional infrastructure investment?

ROI & Value Demonstration

- [ ] Provides measurement framework for time savings, operational efficiency, and risk reduction
- [ ] Can show typical payback period from similar deployments
- [ ] Demonstrates how centralized monitoring reduces need for on-site security staff
- [ ] Shows how investigation time drops (hours to minutes) with unified search and automated incident reports

Pilot & Proof-of-Concept Options

- [ ] Offers pilot deployment to prove value before full commitment
- [ ] Provides clear success metrics and measurement framework for pilots
- [ ] Can demonstrate measurable results within 60-90 days
- [ ] Pilot infrastructure can be expanded (not throw-away investment)

Evidence to Request

- Detailed pricing for representative deployment (specify facility count and camera/door count)
- TCO model showing 5-year costs including hardware refresh, support, and operational expenses
- ROI calculator or case study showing measurable value (time savings, incident response improvement)
- Pilot proposal with success criteria and timeline
- Reference contact information for IT operations staff who can speak to ongoing operational burden and scaling experience

Red Flags

- Pricing is opaque or changes significantly after initial discussions
- Hidden costs emerge (per-feature licensing, professional services dependency, storage overages)
- Cannot articulate ROI in operational terms (hours saved, response time improvements)
- Requires significant upfront infrastructure investment before value is proven
- No pilot option available; requires full enterprise commitment

10. Vendor Viability & Roadmap

Vendor Stability & Investment

- [ ] Company demonstrates financial stability and ongoing R&D investment
- [ ] Has track record of regular product updates and feature releases
- [ ] Shows commitment to public sector market (dedicated team, procurement vehicles, references)
- [ ] Provides clear support model and escalation path for mission-critical issues

Product Roadmap & Innovation

- [ ] Can articulate product direction and upcoming capabilities
- [ ] Demonstrates that existing customers benefit from platform improvements without hardware replacement
- [ ] Shows history of delivering on roadmap commitments
- [ ] Can articulate the relationship between hardware investment and long-term platform value. Does hardware appreciate in capability over time, depreciate, or stay static? Explains how platform architecture supports future capabilities

Differentiation & Market Position

- [ ] Can clearly explain advantages over competitors (legacy on-premise systems, other cloud platforms)
- [ ] Demonstrates technical differentiation, not just marketing claims
- [ ] Has strong position in market segment relevant to your needs (distributed government operations, education, healthcare facilities)
- [ ] References validate differentiation (faster deployment, better integration, superior support)

Exit Strategy & Portability

- [ ] Provides clear data export capabilities (video, access logs, configuration)
- [ ] Explains migration path if you need to change vendors
- [ ] Uses standard protocols and formats where possible
- [ ] Can demonstrate customer examples of smooth transitions (onboarding or offboarding)

Evidence to Request

- Roadmap overview with recent feature releases and upcoming capabilities
- Financial stability indicators (customer count growth, funding, market position)
- References discussing vendor responsiveness, support quality, and roadmap delivery

Red Flags

- Roadmap is vague or has history of missed commitments
- Company financials raise sustainability concerns
- Cannot articulate clear differentiation from competitors
- Vendor lock-in through proprietary formats or lack of export capabilities
- References report poor support or unresponsive vendor

How To Apply This Checklist

Step 1.

Initial Screening (Eliminate Poor Fits)

Use sections 1, 2, and 6 to quickly eliminate platforms that lack basic qualifications:

- Public sector readiness (compliance, procurement access, relevant experience)
- Architecture fundamentals (unified platform versus loosely connected point solutions)
- Deployment realities (timeline, infrastructure requirements, operational burden)

Step 2.

Technical Deep Dive (Validate Core Capabilities)

Use sections 3, 4, and 5 to assess whether the platform delivers on operational requirements:

- Emergency response speed and coordination across systems
- Distributed operations and scalability across your facility footprint
- Investigation tools and evidence compilation suitable for your needs

Step 3.

Operational Fit (Adoption & Sustainability)

Use sections 7 and 8 to evaluate whether the platform will be used effectively:

- User experience and adoption potential with your actual staff
- Governance and compliance alignment with oversight requirements

Step 4.

Commercial Evaluation (TCO & Value)

Use section 9 to validate pricing, TCO, and ROI:

- Price transparency and budget alignment
- Total cost of ownership over 5+ years
- Measurable value demonstration through pilot

Step 5.

Strategic Assessment (Long-Term Viability)

Use section 10 to assess vendor and platform sustainability:

- Vendor stability and market position
- Product roadmap and innovation trajectory
- Exit strategy and data portability

Step 6.

Comparative Scoring

Create a scorecard assigning points for each criterion that matters most to your situation. Weight heavily the factors that address your most critical operational challenges:

- If emergency response time is paramount, prioritize section 3 criteria
- If distributed operations across many facilities is your challenge, weight section 4 heavily
- If budget constraints require phased deployment, focus on section 9 evaluation

Final Guidance

The best platforms will welcome detailed questions and provide concrete evidence. If a vendor resists technical scrutiny, cannot produce references with measurable results, or deflects when asked about limitations and tradeoffs, that tells you something important.

The right platform will be transparent about architecture, honest about what it can and cannot do, and able to demonstrate measurable operational improvements in environments similar to yours.

The Emergency Response Readiness Test

Can your security team lock down an entire facility, share live video with first responders, and coordinate emergency response from wherever they are, right now? If the answer requires qualifications, manual coordination across multiple systems, or IT support, that platform doesn't match your operational reality.

Emergency response speed, distributed operations capability, and operational efficiency aren't features to optimize later. They reflect core architectural choices made years ago. Evaluate whether the platform's architecture aligns with how security operations actually work in government facilities.

The Operational Reality Check

When comparing platforms with different operational models, speak directly with IT operations staff at reference sites, not just security leadership. Ask them:

- How many staff hours per month go toward routine maintenance, updates, and troubleshooting?
- What did it take to scale from pilot to full deployment across multiple facilities?
- Has the operational burden increased, decreased, or stayed constant as you've scaled?
- What unexpected operational costs emerged after the first year?

Platforms may offer similar features on paper, but create very different operational realities. Reference verification with operations staff reveals these differences.

REDLEIF