



REQUEST FOR INFORMATION

RFI #2026-01

NYS DEPARTMENT OF FINANCIAL SERVICES (DEPARTMENT) CENTRALIZED PHYSICAL SECURITY SYSTEM



I. OVERVIEW AND MISSION

The Department regulates insurance, banking, and other financial services with the goal of promoting robust financial services in New York, while safeguarding against financial crisis and protecting both consumers and the industry from fraud. The Department was established on October 3, 2011, with the consolidation of the former Insurance and Banking Departments. The consolidation helped centralize and modernize regulation, enabling New York to keep pace with rapidly innovating financial markets.

II. PURPOSE

The purpose of this Request for Information (RFI) is to obtain market information and industry best practices related to a centralized physical security system that can operate across multiple government offices statewide. The Department is seeking insight from qualified vendors regarding newer, more innovative and cost-effective centralized, agency-controlled physical security system solutions that offer a full complement of features and options which includes, but not limited to:

- credential and visitor management,
- electronic access control,
- video surveillance with on-demand, user-friendly remote viewing capability,
- single, hosted platform,
- system scalability and enhancement,
- State and building security access integration,
- lease agreement and records retention adherence, and
- State IT and cybersecurity compliance.

The Department is located in state-owned and leased buildings throughout the state, including its headquarters in New York City (NYC), a larger office in Albany and smaller satellite suites in Syracuse, Rochester, Buffalo and Garden City. The Department takes a multi-layered approach to security which includes State-owned or landlord-managed building site security as well as Department security systems and efforts.



III. GUIDANCE FOR RESPONDENTS

This RFI is not intended to be an Invitation for Bid or Request for Proposal; therefore, do not include specific cost information in your response beyond what is requested in this RFI.

A. RESPONSE DESIGNATED CONTACT

Name: Rohan Sood / Ron Wachenheim
Email: RFP@dfs.ny.gov

B. SCHEDULE OF DATES

- Department Release of RFI: May 5, 2026
- Questions to this RFI Due: May 12, 2026 at 3:00 PM Eastern Time (ET)
- Answers will be released by: May 18, 2026
- RFI Responses Due: May 29, 2026 at 3:00 PM ET

Please note that RFI schedule dates may change.

IV. RESPONSE REQUIREMENTS

A. RESPONSE CHECKLIST

All the following items are requested to be included in response to this RFI as attached PDF documents:

- Cover letter including:
 - Contact information
- Proposed approaches, and/or other relevant documents from dealings with other New York State agencies
- Answers to Attachment 1 - RFI Questions; and
- Estimate of the cost based on the criteria.



ATTACHMENT 1 – RFI QUESTIONS

STRUCTURE FOR PROVIDING INFORMATION FOR NYS DEPARTMENT OF FINANCIAL SERVICES CENTRALIZED PHYSICAL SECURITY SYSTEM

| | Department Questions | Respondent Answer |
|----------|---|-------------------|
| A | General System and Architecture | |
| 1 | Provide an overview of potential security system solution(s), and their key advantages and challenges. | |
| 2 | What security system components do you recommend for government offices in state-owned or leased buildings where there are varying levels of building security at each location (turnstiles, security desks, etc.)? Explain how the security system integrates these components. <ul style="list-style-type: none"> • Access Control Systems (ACS or “Card Access”) • Video Surveillance (CCTV) • Intrusion and Motion Detection System (IDS or “Burglar Alarm” and Motion Detection) • Duress System (“Panic Buttons”) | |
| 3 | Describe system architecture options (hosted, non-hosted, hybrid) for managing multiple sites under a single platform, including their benefits and drawbacks. | |
| 4 | What level of scalability and future expansion should be considered, and your recommended approach for handling? | |
| 5 | What is your process for conducting a risk assessment to determine what equipment and coverage are needed? Provide a proposed plan, including detailed steps and timeframes. | |
| B | Camera and Video Surveillance | |
| 1 | What camera specifications (resolution, coverage, analytics) are considered best practice for state government offices? | |
| 2 | Illustrate how both live and recorded camera feeds coexist in the same User Interface (UI) as physical access events (badge swipes, door status). Include screenshots or diagrams if possible. | |
| 3 | How is video footage able to be viewed (secure, remotely, on demand, user-friendly)? | |
| 4 | How should video footage be stored (on-site, cloud, hybrid)? | |
| 5 | What retention policies are recommended for compliance and security? Are you able to retain footage for 30 days? | |



| | | |
|--|--|--|
| 6 | What are your recommendations for camera placement and locations (entrances, exits, hallways, elevator lobbies, stairwells)? Advise how these are scalable. | |
| C Access Control | | |
| 1 | What hardware and management software do you recommend for access control? How can it be accessed (on-premises, remotely)? | |
| 2 | How does the system credential access, including managing different levels of access for employees, contractors, and visitors? | |
| 3 | What integration options are available for existing card/device systems? Does that include iClass or compatible cards/devices? For example, explain if/how the card/devices can integrate with the IClass cards used by the NYS Office of General Services to access to its state-owned buildings. | |
| D Integration with Existing Systems | | |
| 1 | How can a new security system integrate with DFS's current multi-layered approach to security which includes state or landlord managed building site security as well as Department security systems and efforts? | |
| 2 | How do you recommend handling existing equipment or wiring? Would you perform any necessary de-installation? | |
| 3 | What challenges typically arise when merging old and new systems, and how would you suggest addressing them? | |
| 4 | What best practices ensure seamless integration with existing hardware and software? | |
| E Intrusion and Motion Detection, and Alarm Systems | | |
| 1 | What sensors or technologies should be considered for intrusion and motion detection? | |
| 2 | How should alarms be monitored and managed (on-site, third-party monitoring, integration with law enforcement)? | |
| 3 | What are your protocols for when an intrusion or motion is detected and/or an alarm is triggered? When is law enforcement contacted and dispatched? | |
| F Visitor Management | | |
| 1 | What technologies are recommended for visitor registration and tracking? | |
| 2 | How should visitor access be restricted and monitored? | |
| G Hardware Components and Compatibility | | |
| 1 | Provide a recommended Hardware List, including but limited to: <ul style="list-style-type: none"> • POE FIPS validated cameras • POE switch recommendations (models, ports, POE standard) and details on VLAN/trunk requirements • Desktop-based PIV enrollment stations (make/model) • PIV card readers for door entrances (make/model, form-factor, tamper detection capability) | |
| 2 | Specify whether readers require control panels or integration modules. | |



| | | |
|---|---|--|
| 3 | Describe software or middleware required to integrate these hardware components into your unified platform. | |
| 4 | Explain how your solution supports Active Directory integration for user provisioning, de-provisioning, and dynamic role assignment. | |
| H | Maintenance and Support Services | |
| 1 | <p>Warranty and Helpdesk</p> <ul style="list-style-type: none"> Define your standard warranty coverage (hardware, software, installation workmanship) and duration. Describe your options for help desk support models (hours of operation, response times by severity, escalation matrix). Provide sample Service Level Agreement (SLA) terms for uptime (99.9% availability) and typical resolution times for common issues (camera offline, reader failure, enrollment station malfunction). Detail multi-layer strategies for addressing system failures. | |
| 2 | <p>Software Updates and Patch Management</p> <ul style="list-style-type: none"> Describe your patch-management lifecycle: frequency of security patches, feature upgrades, and any maintenance windows that may affect system availability. Explain how updates are validated (staging environment) before production rollout. | |
| 3 | <p>Spare Parts and Hardware Refresh</p> <ul style="list-style-type: none"> Outline your recommended spares inventory for critical hardware (camera modules, card reader components), along with turn-around times for replacement upon failure. Provide options and pricing for end-of-life (EOL) or hardware refresh cycles. | |
| 4 | <p>Training and Documentation</p> <ul style="list-style-type: none"> Describe your training approach: scope (administrators, end users, IT support), format (onsite, remote, train the trainer), and duration. Provide examples or outlines of training materials (slide decks, quick reference guides, video tutorials). Confirm that as-built documentation (network diagrams, internet protocol (IP) addressing, configuration parameters) and standard operating procedures (SOPs) will be delivered upon project completion. | |



| | | |
|---|---|--|
| 5 | Reporting <ul style="list-style-type: none"> Describe event monitoring and logging, real-time alerts and exports, and auditing features. List canned reports that can be generated from the system and provide samples of each. Explain how reports can be customized and provide examples. What support is offered to assist with report generation and customization? | |
| I | Budget and Cost Considerations | |
| 1 | What factors most significantly impact the total cost of ownership (hardware, software, licensing, monitoring)? | |
| 2 | Are there cost-saving strategies without compromising security? | |
| J | Implementation | |
| 1 | What is a typical timeline for all phases of the project (planning, procurement, installation, testing, troubleshooting, etc.)? | |
| 2 | What potential challenges should we anticipate during implementation and how would you suggest addressing them? | |
| K | Additional Information | |
| 1 | How is AI currently being used in system operations and how will its use be expanded in the future? Are there other emerging technologies or best practices we should consider? | |
| 2 | How does the potential security system solution(s) address the unique challenges of multi-tenant buildings where public access areas intersect with restricted, secure state government office spaces? | |
| 3 | Given government offices may be higher-tier targets, how does the potential security system solution(s) address their differing threat levels? | |
| 4 | How does the potential security system design ensure resilience in natural/human-made disasters, extreme weather events and threats unique to urban-based areas? | |