

ITS Strategic Roadmap – FY16

Physical Security Support

Author: *John Griffey*

Date last updated: *1/21/2015*

Background

The physical security of Metropolitan Government facilities is a joint effort across multiple Metro departments, encompassing a range of services. ITS' role is to provide video camera management and controlled physical access to Metro departments and agencies.

These services include

- centralized management of Metro's open source, non-proprietary physical access (cardkey) infrastructure, Lenel OnGuard,
- centralized management of the non-proprietary video camera management system, Milestone, and
- centralized management of the Global Facilities Management Systems (GFMS) key box infrastructure, which provides for secure and auditable access to physical keys.

These services are capable of being integrated with each other as well as Metro's identity management service, which allows Metro users to login to the network and access Metro resources. This allows Metro to better manage who has both logical and physical access to Metro assets.

The General Services department provides a legacy and proprietary physical access (cardkey) system that is used in general government facilities and the Davidson County Sheriff's Office, which was built and managed prior to the implementation of the Lenel OnGuard system.

To effectively manage these services for our customers, we work closely with the other departments and agencies responsible for other aspects of physical security, particularly those that manage security (Davidson County Sheriff's Office) and those that are responsible for planning, construction and maintenance of facilities (General Services departments and contracted construction companies).

The services provided by ITS are consumed by all general government Metro departments and agencies, including the Metro Nashville Police Department, Davidson County Sherriff's Department and the Justice community of departments and agencies. Metro Nashville Public Schools maintains and operates its own separate physical security systems for staff and students.

Current Strategic Drivers

1. **Customer need: video camera management infrastructure** (High) – Several departments have need for in a cost efficient,
2. **Customer need: enterprise key box management** (High) – Several departments have expressed interest in a better, more efficient way to manage and audit physical keys or assets.



3. **Demand for Secure Government Facilities and Systems (High)** – With massive data breaches in the news on seemingly a daily basis, we must strive at all times to protect the security, availability and integrity of all systems and facilities entrusted to our management.
4. **Consolidated Service vs. Multiple One-off Implementations (High)** – There are management and cost benefits from a single Metro Government solution for this service. This must be balanced with the cost-benefit equation when considering conversion of existing systems to roll into the enterprise solution.
5. **Demand for open records/litigation video holds (High)** –public records requests take a considerable amount of time. Currently, some cities, like Seattle, are struggling to meet open records requests of video data due to inefficient methods of redacting and reviewing the data.
6. **Cost Reduction (High)** – The proprietary physical access infrastructure currently in place has become increasingly expensive to support and customers have expressed interest in a more cost-effective solution.

On the Horizon Strategic Drivers

1. **Customers demand: Mobile access to cameras (High)** – Market research shows that many customers mark the ability to consume video footage using mobile devices as a necessity. Some of these mobile devices include remotely controllable devices, such as unmanned aerial vehicles (UAVs).
2. **Short maintenance/life cycle of Security Equipment (High)** – Industry standards of 5% failure rate per year and a 5 year life cycle.

Short Term Goals (0-6 months) 7/1/15 – 12/31/15

#	Goal/Objective	Est. Start	Est. Duration
1	Alarm and Video Integration – The marriage through software of physical access control alarm data and video camera surveillance data to optimize both platforms to a single, searchable record.	7/15	6 months
2	Develop process documentation across all three supported solutions (Lenel, Milestone, and GFMS) and formalize all aspects of these service offerings.	7/15	12 months
3	Rollout of physical security infrastructure that can be used for protecting racks at both new construction and legacy locations.	7/15	12 months
4	Rollout of technology to allow consumption of camera footage from mobile devices.	7/15	9 months
5	Plan and execute system replacement of legacy access control or video equipment, develop documentation of process.	7/15	12 months
6	Research methods and develop processes for providing video data that may be part of open records requests.	7/15	12 months
7	Develop charge back model around all physical security for implementation in budget year FY17.	7/15	6 months



Medium Term Goals (6-18 months) 1/1/16 - 12/31/16

#	Goal/Objective	Est. Start	Est. Duration
1	Rollout of technology to allow consumption of camera footage from mobile devices.	1/16	12 months
2	Develop budgetary estimates for typical system takeover/replacement or upgrade in an effort to provide customers a value-added proposal in place of continued service and maintenance of their proprietary system.	1/16	6 months
3	Develop plan for budgeting for end of life equipment.	1/16	3 months

Long Term Goals (18-36 months) 1/1/17 - 6/30/18

#	Goal/Objective	Est. Start	Est. Duration
1	With cooperation of General Services, perform physical access penetration testing. Capital funding will be required.	1/17	12 months
2	With cooperation of General Services, begin planning for security upgrades/takeovers of legacy equipment as a value-added proposal in place of continued service and maintenance.	1/17	6 months

Related Roadmaps:

- Network Infrastructure
- Network Security
- Structured Cabling

