ITS Strategic Roadmap – FY20 Planning

Physical Security Support

Author: *Betsy Talley*
Date last updated: *December 27, 2018*

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 via cardkey systems to Metro departments and agencies. With the beginning of fiscal budget year 2017, the access control system P2000 and support staff moved to the ITS department which consolidated the support for all Physical Access Control systems. These services include:

- Centralized management of Metro's standard open source, non-proprietary physical access (cardkey) infrastructure, Lenel OnGuard
- Centralized management of Metro's legacy physical access (cardkey) infrastructure, the proprietary P2000 system
- Centralized management of the non-proprietary video camera management system, Milestone
- Centralized management of the Global Facilities Management Systems (GFMS) key box infrastructure, which provides for secure and auditable access to physical keys

Most of these services are integrated with each other as well as Metro's identity management services, 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 P2000 system 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 Sheriff'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. **Demand for Secure Government Facilities and Systems** (High) – There is an increasing need across all government entities to provide additional physical security for staff as well as physical security controls to help protect access to electronic data at rest and during transit.
2. **Customer Demand: Safety cameras** (High) – Many departments are requesting additional camera systems to aid in addressing security concerns.
3. **Consolidated Service** (High) – There are management and cost benefits from Metro Government having an enterprise non-proprietary solution for both physical access and camera systems as well as providing ease of access in a crisis when all of Metro is using the same infrastructure and the system if fully integrated with Active Directory.
4. **Regulatory Requirements** (High) – Public records requests per Sunshine Laws for video can take a considerable amount of time to produce. Additionally, as more cameras are deployed, especially car and body cameras, the requests for video can increase dramatically.
5. **Metro Building Projects** (High) **–** Through new construction and end of life equipment, the proprietary physical access infrastructure is being replaced with the non-proprietary solution.

On the Horizon Strategic Drivers

1. **Industry Trends/Technology Changes** (Medium) – Evolution of video camera and card key capabilities.
2. **Privacy Considerations** (Medium) – As residents learn more about impact to their privacy based on social media and business breaches, as well as from increasingly ubiquitous cameras in public places, the potential for legislation increases.

Short Term Goals (0-6 months) 7/1/19 – 12/31/19

#	Goal/Objective	Est. Start	Est. Duration
1	Plan and execute system replacement of legacy and end of life support access control and video equipment.	7/19	On going
2	Plan and execute system migration of legacy access control (P2000) to enterprise access control (Lenel).	7/19	On going

Medium Term Goals (6-18 months) 1/1/20 – 12/31/20

#	Goal/Objective	Est. Start	Est. Duration
1	Continue system migration of legacy access control (P2000) to enterprise access control (Lenel).	1/20	On going
2	Update and increase the capacity of the physical security infrastructure to support access control demand.	1/20	6 months
3	Update and increase the capacity of the physical security infrastructure to support video camera demand.	1/20	6 months

Long Term Goals (18-36 months) 1/1/21 – 6/30/22

#	Goal/Objective	Est. Start	Est. Duration
1	Continue system migration of legacy access control (P2000) to enterprise access control (Lenel).	1/21	On going
2	Update and increase the capacity of the physical security infrastructure to support access control demand.	1/21	12 months
3	Update and increase the capacity of the physical security infrastructure to support video camera demand.	1/21	12 months

Related Roadmaps

- Network Infrastructure
- Wireless Network Infrastructure
- Structured Cable Management
- Server Support