Middleborough Police – Electronic Security Narrative

1. PURPOSE

The purpose of this document is to define specific security, access control and surveillance requirements for the exterior and interior of the proposed Middleboro Police Station. These requirements should be aligned with the existing Middleboro Police standards.

2. SITE PERIMETER

Fencing

Perimeter fencing around the police station will encompass the entire site and vehicle control barriers will be employed to designate public and private areas of the site. Radio Frequency Identification (RFID) tags will be programmed to open vehicular gates for private parking of patrol and personal vehicles.

Surveillance

Perimeter surveillance will include high resolution, lowlight and infrared fixed cameras, including 180 and 360 degree cameras in concert with video analytics, including motion detection, to establish a virtual perimeter and monitor activity within the site. Surveillance will be used to cover the vehicular entrances of the site, visitor and employee parking areas, main and exit only doors. Cameras will be aesthetically mounted to light poles, if required, and the facility, where permitted, in order to provide maximum coverage of the perimeter. All exterior building cameras will be power over Ethernet (PoE), specified for the environment in which they are located and will include lightening and surge protection. All PoE power supplies will be on Uninterruptible Power Supply (UPS) and emergency power. Pole mounted cameras, if required, will be powered from independent 120VAC power supplies mounted in a National Electrical Manufacturers Association NEMA enclosure at the base of the pole.

The benefit of utilizing a PoE solution not only supplies low voltage power rather than high voltage power to these devices, but more importantly provides the means to control power to the device. Central control of the PoE devices allows for devices to be turned on or off based on a predetermined schedule, a sensor, or an event, such as motion detection. The result can be reduced consumption of power to devices, reduced power usage and a greener building. In addition, PoE reduces the use of materials, eliminating the need to provide a power cable to the device.

3. BUILDING PERIMETER

The proposed facility has specific entry doors for visitors and employees, all of which will be controlled by a proximity card reader, door position switch and monitored by surveillance both on the interior and exterior. The visitor entry door will include 2-way audio and video communication with the dispatch area through the use of a video intercom system whereby a visitor would request access into the facility. A master intercom station mounted at the desks inside the Communications Room will be programmed with the functionality to electronically unlock the door if access is granted.

The doors associated with the Lobby, Sallyport and Mantrap will be interlocked so as not to allow more than 1 door to be open at a time. These doors will be controlled through the access control system with override capability from Communications.

All exterior doors not used for normal entry, but for emergency egress only, will be equipped with hardware only on the interior side of the door, door position switches and audible alarms. Alarms will be generated for unauthorized access and can be silent alarms, generated only on the access control workstation, and/or audible alarms for local annunciation.

4. BUILDING INTERIOR

Access Control

All controlled and monitored doors will communicate with wall mounted access control panels mounted in a climate-controlled room inside the facility. This location will also house the PoE switches that power the cameras and the video management system server. These panels will transmit the access control data to an access control system, controlled through a workstation, located in Communications and, if required, other locations in the facility. The system will have the capability to receive and acknowledge various types of facility alarm conditions to include door-propped-open and door-forced open. For ease in identifying the locations of alarms, all events will be displayed on a facility map indicating the specific location and type of alarm.

Through the access control system and associated door controlling equipment, Communications will have the capability to unlock electronically controlled doors as well as lockdown the facility, rendering all card access doors only to be operated by pre-authorized credentials. These panels will also include a fire alarm module to support a connection with the fire alarm system.

The access control system database will be linked to the human resource database, which will allow new employee data to be passed to the system for pre-population of card holder data, which will allow personnel to quickly create new access control credentials. Access control credentials will be produced with badging software within, or integrated with, the access control system and allow for multi-colored badges with a photograph and permit full user design of style, logo, fonts and data placement. The system will be part of, or integrated with, the access control system in order to permit tracking of individual badge usage, activation/deactivation of badges at any time or based upon user defined rule sets, and provide both standard and custom reporting capability.

Card access will be employed at the following locations (see diagram for specific locations and in/out readers):

A. Vestibule
B. MIRCS
C. Interview Rooms
D. Corridors leading from the Lobby
E. Communications
F. IT/E911

G. NSO
H. Corridor from Training
I. Man Trap
J. Processing
K. Sally Port
L. Evidence Processing
M. Evidence Storage
N. Drugs
O. Electrical
P. Emergency Electrical
Q. Storage
R. Passage

Video Management System

The video management system will be capable of recording and storing all video, including the exterior cameras, for a minimum of 30 days at high definition resolution. The video management system will transmit video to a video management workstation located in Communications, and/or at alternate locations, where live viewing will be permitted of any camera image. All cameras will be capable of transmitting in color and exterior cameras will have low light capability where needed (based upon lighting design and configuration). Software for motion based as well as object based and/or forensic video detection will be used in order to provide discrimination of unwanted versus normal events. Interior cameras will be powered via PoE.

Surveillance cameras will be vandal resistant and employed at entry doors from the exterior and interior doors leading from public spaces into private spaces. Cell cameras will utilize audio analytics to trigger an alarm when a decibel threshold is exceeded. Interview Room cameras will have visibility of the rooms' door, compliant with regulations and can include an integrated microphone for audio recording. Interview Room cameras will also require recording at 30 frames per second for matching up seamlessly with the recorded audio. All other cameras will require a maximum of 15 frames per second.

Electronic Control Equipment

Each desk in the Communication Room will have a workstation for the access control system, the video management system, a master video intercom, lockdown button and duress button. Each desk will also include a door controller keypad with override buttons for the Sallyport overhead doors, Cell Doors, Lobby doors and other doors requiring electronic override. Although functionality through the access control system can be used for this purpose, a programmed keypad will allow easy access to override typically overridden doors. Additionally, an area in Communications Room will be used to badge employees and will include the badging camera and ID printer.

Above the transaction window in the Communications Room, four (4) large screen monitors will continuously run video feeds from the interior and exterior cameras as well as live television, including local news and weather. These monitors will be in addition to the workstations and

monitors at each dispatch desk that will be used to enlarge single views and review transactions from the access control system.

Speakers and Volume Control
IP speakers will be distributed throughout the facility for integration into the radio system amplifier. Audio control of these speakers will be provided in specific offices and conference rooms. See attached diagrams for speaker locations and areas with volume control.

2-Way Intercom Communication
Each cell will include audio only communication with staff members who have master intercom stations. The cell intercoms will be wall recessed mounted and vandal resistant.

5. INFRASTRUCTURE

Below are the various power, network and conduit requirements for the access control and video assessment systems:

Network:

A. A network connection would be required for each access control panel location. This is typically in the form of a network jack located within the security equipment enclosure.
B. Category cabling will be required for each camera, routed back to a network switch inside a secure closet.
C. Two (2) network connections would be required for each video server recorder; the final configuration for recorders will vary depending on the number of cameras. For most designs, a network switch is installed in one or more of the security equipment racks for the purpose of connecting video servers and mass storage devices.
D. Coordination of IT elements such as data drops, IP addresses and VLAN configuration, if desired, will be conducted well in advance of system deployment and will be closely monitored throughout the system installation.
E. A network connection would be required for each access control, video management, and visitor management workstation.
F. Rack mounted network equipment will be installed in a seven (7) foot server cabinet with locking system.

Power and Fire Alarm:

Power for security devices, as outlined below, should not be shared with any circuit supplying non-security related equipment.

A. Provide one (1) 120VAC 20 Amp UPS circuit and Fire Alarm connection for each access control panel location.
B. Provide one (1) 120VAC 20 Amp UPS circuit for each door to receive an electrified panic hardware device. This circuit may be shared with other security devices.
C. Provide one (1) 120VAC 20 Amp UPS circuit and Fire Alarm connection for each door to receive any type of delayed egress device. This circuit may be shared with other security devices.
D. Provide one (1) 120VAC 20 Amp UPS circuit and Fire Alarm connection for each set of interlocked controlled doors. This circuit may be shared with other security devices.

E. Provide 120VAC UPS power for each pole mounted exterior camera. This circuit may be shared with other security devices.
F. Five (5) 120VAC 20 amp UPS circuits would be required for each desk inside Communications.
G. Six (6) 120VAC 20 amp UPS circuits would be required to support the security desk monitors.
H. A rack mounted managed UPS with have adequate power to support at least four (4) hours of outage in the event of a power loss for all rack-mounted equipment.

Conduit:

A. One (1) 1" conduit would be required for each card reader location. Conduit should be run from the card reader location to the nearest IT closet or cable tray.
B. One (1) ¾" conduit would be required for the following devices and would be run to the nearest IT closet or cable tray:
    1. Video assessment camera
    2. Monitored doors without a card reader
    3. Intercom or Call for Assistance stations