CHAPTER FIVE

GUIDELINES ON ACCESS CONTROL, SCREENING & MONITORING

Access control, screening, and monitoring systems can play an integral role in securing a building and its immediate surroundings. Access control systems limit who can enter a building; screening systems limit what can enter a building; and monitoring systems observe the people and things in and around a building. This chapter outlines various recommendations for the use of such systems to enable them to deter terrorist attacks and generally improve building security.

Access Control Systems

To mitigate the risks associated with terrorist penetration of buildings, the NYPD recommends that owners of Medium and High Tier buildings implement access control systems. As a rule, building owners should design access control systems that do not obstruct or impede egress or emergency evacuation. For the purposes of access control, the NYPD distinguishes between buildings with controllable population flows and buildings with inherently non-controllable population flows. The latter category encompasses transportation hubs that accommodate large volumes of travelers and visitors.

The recommendations presented in this section fall into two general categories: those related to general building access and access to sensitive areas, including parking garages and locations with large pedestrian populations; and those related to sensitive security information and critical facilities, such as rooms housing electrical, mechanical, and telecommunications equipment. The former apply only to buildings with controllable population flows, and the latter apply equally to buildings with controllable and non-controllable population flows.

General Building Access and Access to Sensitive Areas

Access control systems keep track of who enters and exits a building. On the most basic level, these systems distinguish between building "insiders" – including tenants and employees – and building "outsiders" – including invited guests and the general public. The NYPD created the following recommendations to address the threat from unknown, potentially dangerous "outsiders."

For High Tier buildings, the NYPD recommends the implementation of access control systems that incorporate identity authentication and turnstiles to enforce entry authorization. "Insiders" should access High Tier buildings using access control cards, biometric devices, or badges that support multi-layered technology (e.g., smart cards with biometrics); and "outsiders" should access these buildings using time-sensitive temporary passes or proxy cards. Additionally, the NYPD recommends that these systems limit access to sensitive areas within High Tier buildings based on personnel category (e.g., tenant, non-tenant employee, visitor, general public, etc.). Owners of High Tier buildings should configure access control systems to comply with the NIST standards issued pursuant to Homeland Security Presidential Directive 12 to rapidly and electronically authenticate secure, reliable forms of identification.[1]

For Medium Tier buildings, the NYPD recommends the implementation of perimeter access controls, such as badge or identification card systems, to quickly process "insiders" at all entrances and exits. "Outsiders" should access Medium Tier buildings using temporary guest passes, and security personnel should continually man security stations within the building, with open sight lines to entry and exit points to allow effective monitoring by security personnel.

Although the NYPD tailored the preceding recommendations to meet the specific security needs of Medium Tier buildings, owners of Low Tier buildings who desire to implement access control systems may find these recommendations useful. Regardless, security personnel at Low Tier buildings should develop standard operating procedures and protocols for access control that can be implemented pursuant to an incident or at elevated threat levels.

Access to Critical Facilities and Sensitive Security Information

Although access control systems may effectively mitigate the threat to buildings from "outsiders," history has demonstrated the potential for "insider" exploitation of building vulnerabilities and sabotage. For example, in March 2004, British authorities disrupted a homegrown terrorist cell planning to use 1,300 pounds of ammonium nitrate fertilizer to launch one or more unspecified attacks in Britain. While employed as a sub-contractor for the Transco gas company, one of the cell members, Waheed Mahmood, stole sensitive CD-ROMs that detailed the layout of gas pipelines in southeast England.[2] In a separate incident in 2007, British authorities arrested Omar Rehman, who took a job working at a hotel in order to obtain security system plans and diagrams of security posts.[3]

Owners of Medium and High Tier buildings should establish control mechanisms to ensure that terrorists do not gain access to certain documents, including those containing sensitive security information, which may be used to exploit specific vulnerabilities and in attack planning. The NYPD recommends that owners of Medium and High Tier buildings limit access to blueprints and floor plans, and that all building owners further limit access to documents containing sensitive security information. This may be accomplished by establishing requirements for storage, disclosure, reproduction, transmission, shipment, disposition, and labeling of these documents. Additionally, owners of Medium and High Tier buildings should allow access to documents containing sensitive security information only on an as-needed basis, and should conduct background checks on all individuals granted such access.

For Medium and High Tier buildings, the NYPD recommends that access control systems limit access to critical facilities, including building security, building engineering, and fire-control rooms. Accordingly, security personnel in High Tier buildings should conduct background checks on all individuals with access to critical facilities both during and after construction, with recurring screenings of individuals involved with critical building functions. For Medium Tier buildings, the NYPD recommends that security personnel conduct background checks on all post-construction employees with access to critical facilities. To the extent possible, access to critical facilities in Medium and High Tier buildings should only be granted on an as-needed basis.

Screening Systems

To mitigate the risks associated with explosive or other devices detonated within a building, the NYPD recommends that owners of Medium and High Tier buildings with controllable population flows implement screening systems. The NYPD's recommendations relating to screening systems span three general categories: people and hand-held bags, delivered packages, and vehicles. The NYPD's recommendation for screening threshold levels applies equally to all three categories.

Generally, the level to which security personnel should screen for explosives depends on the DBT levels for threats from a contact charge, measured in TNT-equivalency, of the building's structural columns. To ensure that an attack from within a building does not result in its collapse, the NYPD recommends that owners of High Tier buildings set screening thresholds at levels no higher than the DBT level for threats from a contact charge on a structural column. For example, if the DBT level of structural columns in a garage is 90-pounds TNT-equivalent, all persons, packages, and vehicles accessing that garage should be screened such that no bomb with a 90-pound TNT-equivalent yield or larger can gain access. This recommendation represents only a minimum standard: owners of High Tier buildings should consider setting screening thresholds at levels significantly lower than determined DBT levels for threats from a contact charge on structural columns.

With respect to people and their hand-held bags, the NYPD recommendations distinguish between screening "insiders" and "outsiders." For High Tier buildings, "outsiders" should pass through magnetometers and their bags should be x-rayed; "insiders" need not pass through magnetometers, but their bags should be subject to search. Beyond these minimum standards, owners of High Tier buildings should consider the use of additional screening technologies, including walk-through explosives detection portals and radiation detector portals or pagers. The

Magnetometers and x-ray machines screen people and their hand-held bags.

NYPD also recommends that owners of High Tier buildings create secondary screening areas where security personnel can resolve anomalies using explosive trace detection equipment, handheld magnetometers, pat downs, and manual searches.[4] For Medium Tier buildings, the NYPD recommends that security personnel x-ray all "outsiders'" bags upon entry and store magnetometers on-site for use as circumstances require.

With respect to delivered packages, the NYPD recommends universal screening at Medium and High Tier buildings with stationary x-ray equipment and explosives detection canines or equipment. Building owners should post signage, indicating that all packages are subject to search. The NYPD also recommends that security personnel at Medium and High Tier buildings develop package screening standard operating procedures and protocols that can be implemented pursuant to an incident or at elevated threat levels.

With respect to vehicles, the NYPD recommends screening for High Tier buildings at direct entry points as well as at the entrances to underground parking areas and loading docks. Effective vehicle screening requires an adequate number of well-lit vehicle entrances to accommodate peak flows of vehicular traffic and to provide sufficient visibility of vehicles at the true perimeter.[5] The NYPD recommends that security personnel at High Tier buildings ensure that vehicle access points are securely locked when not operational, illuminated during off-hours, and inspected periodically by a roving patrol. Additionally, barrier systems should be put in place to thwart any attempt to "rush" the checkpoint.[6]

The NYPD recommends that owners of High Tier buildings provide for off-site screening of vehicles;[7] when no such design is feasible, building owners should create hardened on-site areas sufficiently removed from critical facilities and occupied spaces. Because underground parking areas and loading docks may create significant vulnerabilities based on their proximity to the base of a building, owners of High Tier buildings should harden them as much as possible, and design them to both limit damage to adjacent areas and vent explosive forces outward.[8] The NYPD recommends that Medium Tier buildings maintain signage noting that all vehicles are subject to search.

In all areas used for screening of people and their hand-held bags, delivered packages, and vehicles, lighting levels should conform to the standards set by the Illuminating Engineers Society of North America.[9]

To ensure both expediency and efficacy in all parts of the screening process and in all screening categories, security personnel at High Tier buildings should receive training that goes beyond the basic requirements needed to perform their functions. In certain instances, local law enforcement presence combined with judicious deployment of facility K-9 teams may be used to augment security staff capabilities. In general, system designers at High Tier buildings should consider and incorporate all appropriate screening technologies.[10]

Monitoring Systems

Monitoring systems can play an important role in protecting a building from terrorist attack. For example, an effective monitoring system may deter terrorists conducting reconnaissance from targeting a building. Monitoring capabilities, such as closed-circuit television (CCTV) systems, give security personnel enhanced domain awareness and improve their ability to detect suspicious activity. Monitoring systems may also serve as an important tool for investigating attacks, crimes, and other security incidents after they occur.

Sophisticated terrorists will take the existence of monitoring systems into consideration when conducting pre-attack planning and assessing operational risk. For instance, between 2000 and 2004, Dhiren Barot (a.k.a. Issa al-Hindi) carefully scrutinized the positions and features of CCTV cameras while conducting surveillance missions in the United States. While casing the New York Stock Exchange, he reported in his notes that, "there are round, tinted opaque (black) glass ones [CCTV cameras] – thus allowing freedom of rotation without public knowledge of which direction they are turning… it should never be assumed that all the cameras have been accounted for as there may be hidden cameras." Barot even acknowledged in his notes that he, "took many chances" in conducting such overt reconnaissance.[11]

The NYPD recommends that owners of Medium and High Tier buildings install comprehensive CCTV systems. All other buildings planning to install CCTV systems or security lighting should also follow the NYPD recommendations described in this chapter.

Furthermore, owners of buildings utilizing CCTV systems should post signage stating that the area is being monitored for security purposes.

CCTV cameras in many shapes and sizes.

Incorporating CCTV systems into a security plan requires state-of-the-art technology as well as well-trained personnel to monitor and operate the cameras. The NYPD recommends that security personnel at High Tier buildings establish monitoring posts with detailed operating instructions. Monitoring personnel should not be assigned any additional duties and should be rotated intermittently between 30 minutes and one hour to avoid end-user fatigue.[12] Implementing robust monitoring practices increases the likelihood that security personnel will detect suspicious behavior. Monitoring personnel and other security personnel should bear in mind that terrorists change tactics in order to outmaneuver static defenses. For instance, based on his observation that limousines are common in commercial districts with large numbers of corporate executives, Barot developed the "Gas Limos Plot" to detonate gas cylinders packed in as many as three limousines parked in the underground garages of various targets.[13]

The NYPD recommends that owners of Medium and High Tier buildings implement comprehensive CCTV camera coverage in critical facilities and sensitive areas within and around buildings, operated 24 hours a day. All CCTV cameras should be Underwriters Laboratories-listed to ensure that the devices are electrically sound and properly grounded to avoid shock and fire hazards; and FCC-compliant to ensure that the devices do not create interference with other electronic components utilized in the building.

Additionally, the NYPD recommends that building owners take steps to prevent tampering with CCTV systems and their associated video signals, including: installing cables and wires in a manner that will prevent unauthorized access;

transmitting video signals via secure mediums; positioning exterior CCTV cameras at high elevations; and placing pan-tilt-zoom and fixed cameras in tamper- and weather-resistant housings.

In positioning CCTV cameras, systems installers at Medium and High Tier buildings should avoid blind spots and use proper lighting to ensure clear visibility. To avoid a "washout" of the image until excess light is dimmed or removed, systems installers should seek to minimize the direct exposure of CCTV camera lenses to light. Additionally, the NYPD recommends that owners of High Tier buildings ensure that lighting for CCTV systems is proprietary and under the exclusive control of building personnel. Lighting should be operated by an automatic photocell controller or timing circuit to provide an extension of daylight hours and guard against human error. Additionally, to ease transitions on pan-tilt-zoom cameras, the NYPD recommends that owners of High Tier buildings ensure uniformity of lighting throughout a site.

To the extent that video from CCTV cameras is to be used for purposes beyond real-time viewing, the NYPD recommends that it be recorded at a speed of no less than 15 frames per second; and at an image size of no less than 2 CIF. Recorded video should be archived for a minimum of one month for review of security incidents not immediately evident.

Additionally, the NYPD recommends that owners of High Tier buildings ensure that CCTV systems are interfaced with current alarm points and access control systems to allow for remote assessment of alarm conditions. CCTV cameras should be specified with alarm and incident presets and should be programmed to automatically focus on the point in alarm.

NYPD Lower Manhattan Security Coordination Center

Looking to the future, it will increasingly be possible to network CCTV systems to local law enforcement coordination centers. Multiple cities have begun to introduce such cutting-edge integrated security systems. For example, in the

Box 9: Lower Manhattan Security Initiative

In order to help ensure public safety and security and to detect, deter, and prevent potential terrorist activities, the NYPD developed the Lower Manhattan Security Initiative (LMSI), a networked domain awareness project covering 1.7 square miles of Manhattan, from Canal Street to Battery Park, and from river to river. As part of this effort, the NYPD has partnered with several Stakeholders, including numerous public agencies and private companies, located in Lower Manhattan.

LMSI's integrated approach to security consists of an increased patrol presence on the streets, and the use of domain awareness technologies deployed in public areas, including CCTVs owned by the NYPD and the LMSI Stakeholders, LPRs, and chemical, biological, radiological, and nuclear detectors. The technologies are networked and supply critical supplemental assistance to officers' ongoing security and public safety efforts.

The Lower Manhattan Security Coordination Center, which serves as the aggregation point for data gathered by officers and the various domain awareness technologies deployed as part of LMSI, opened on October 31, 2008. It is staffed by uniformed members of the NYPD Counterterrorism Bureau and has workstations for representatives from the various public and private Stakeholders.

fall of 2008, the NYPD opened a state-of-the-art coordination center in Lower Manhattan in cooperation with private stakeholders and federal, state, and local government partners. The coordination center furthers the NYPD's efforts to detect, deter, and prevent potential terrorist activities by integrating data collected by CCTV cameras, license plate readers (LPRs), and other domain-awareness technologies. The cities of London and Chicago have also introduced advanced domain awareness systems with coordination centers for information collection.[14] The integration of private CCTV systems into law enforcement coordination centers supplies critical supplemental assistance to officers' ongoing security and public safety efforts, and enhances the collaborative nature of those efforts by leveraging the resources of the private sector.