SENSITIVE INFORMATION

Security Assessment Report

Company HQ

Department Solutions
9111 Falmouth Ave
Playa Del Rey, CA, 90293

Assessment Date: January 21, 2026
Presented by:
Secure Core LLC

1660 East Central Ave
Los Angeles, CA 90402 P. 310-413-6712
Assessor: Jessie James, Security Director

Table of Contents

BACKGROUND

Scope

On Jan. 21, 2026, Secure Core LLC, conducted a Security assessment at Company HQ located at the following address: 9111 Falmouth Ave, Playa Del Rey, CA, 90293.

Based on the visual inspection conducted of the facility, surrounding property, general utilities and infrastructure, this security assessment serves to identify critical physical and procedural vulnerabilities to provide stakeholders with common mitigation solutions for consideration. The primary focus of this report is on physical security and crime prevention through environmental design. Although this report references elements regarding building safety, ADA compliance or fire hazard prevention, it is beyond the scope of this report and should be addressed respectively. The observations made by the assessor and presented in this report are based on industry standard references, best practices, acquired knowledge and the assessor's professional experience in efforts to tailor the suggested mitigation options to the physical and operational needs of the facility. Solutions for consideration listed within the report do not necessarily include every option available, but rather present some of the most common options employed within the security industry. Unless stated otherwise this security assessment does not include any aspect of IT/ Cyber vulnerabilities which should be assessed independently.

Disclaimer

Any action taken by a recipient of this report or by his/her representatives based upon this security assessment does not guarantee nor warrant in any way whatsoever that the assessed location/s, facility, its users or visitors may or may not be rendered safer, invulnerable or in any fashion impervious to successful penetration, attack or other act which could cause property damage and/or personal injury to the facility or its patrons.

By accepting this security assessment report, and or by taking or avoiding to take any action based on its written or verbal content, Company HQ hereby agrees to RELEASE, WAIVE, DISCHARGE, HOLD HARMLESS and NOT SUE Secure Core LLC, any of its officers and or employees, for any and all loss, harm, liability or damage caused as a consequence of the security assessment, release of the written report, pictures and assessors' opinion including any loss arising from a claim of negligence. Further, by accepting this report, Company HQ agrees to INDEMNIFY Secure

Core LLC, its agents, officers and employees from any loss, harm, liability, lawsuits, damages or costs, including court costs and attorney fees.

EXECUTIVE SUMMARY

Overall, the facility demonstrates a Moderate level of physical security. Critical assets are generally well protected; however, gaps in perimeter control and visitor management expose the facility to potential unauthorized access or theft.

Positive findings will be added by the assessor after review.

Key Findings

- Lack of adequate perimeter fencing - The existing fencing does not sufficiently deter unauthorized entry.

- Inconsistent visitor management protocols - Procedures for verifying and tracking visitors are not uniformly enforced.

- Limited surveillance coverage - Certain areas of the facility lack adequate CCTV monitoring.

These findings represent areas where the facility's current controls may not fully align with best practices or organizational security objectives.

Recommendations

- Immediate / High Priority: Repair perimeter fencing and ensure gate locks are functional.

- Medium-Term / Moderate Priority: Implement enhanced visitor verification and escort procedures.

- Long-Term / Strategic Priority: Upgrade CCTV system for full coverage and integrate with access control.

Conclusion and Next Steps

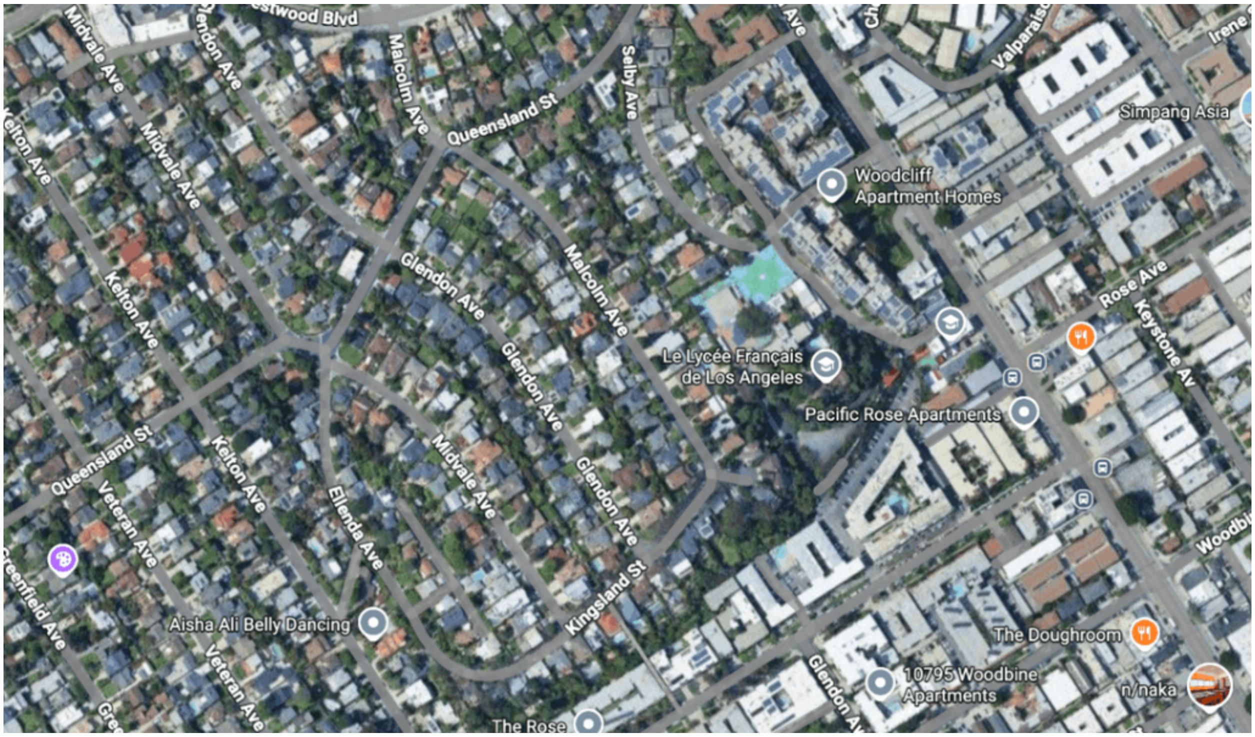
This assessment provides a roadmap for improving physical security across the facility. Implementing the recommended measures will significantly reduce risk exposure, strengthen deterrence and detection capabilities, and improve overall resilience. It is advised that management develop an action plan assigning responsibilities, timelines, and resources to ensure timely remediation.

CRIME ANALYSIS

The geographic scope of this crime and threat analysis encompasses a defined radius around the Company HQ located at 9111 Falmouth Ave, Playa Del Rey, CA 90293. The data methodology involves a comprehensive review of open-source information, leveraging various reliable sources to ensure the accuracy and relevance of the findings. These sources include the FBI Uniform Crime Reporting (UCR) Program, the National Incident-Based Reporting System (NIBRS), reports from the Department of Homeland Security (DHS), the Department of Justice (DOJ), state and local police databases, academic research, and credible news outlets.

Neighborhood Profile

The neighborhood surrounding the Company HQ features a diverse demographic landscape. The population is characterized by a mixture of families and young professionals, with median income levels reflecting the economic dynamism of the area. Housing options range from single-family homes to multi-unit dwellings, catering to a variety of socioeconomic statuses.



The physical environment is shaped by several factors, including land use designated for residential, commercial, and recreational purposes. Public transit routes provide accessibility, with bus lines connecting to major urban centers. The area boasts adequate lighting in public spaces, and its proximity to essential services such as police stations and hospitals enhances community safety.

In terms of historical crime context, the area has experienced fluctuations in crime rates over time, influenced by socioeconomic factors. Notable past incidents, including violent crimes and property offenses, have shaped local perceptions of safety and security.

Executive Summary of Key Findings

The analysis reveals significant trends in crime rates, with property crime rates showing a notable increase in the past year, alongside a stable incidence of violent crime. Noteworthy geographic hotspots for crime have been identified, particularly in areas with high foot traffic. Temporal patterns indicate that most crimes occur during late-night hours, especially on weekends, while emerging trends suggest a rise in online-related offenses. The presence of extremist groups and potential for civil unrest has been historically low, though recent tensions in the broader socio-political climate warrant attention.

Crime Data Analysis

The major crime categories within the vicinity include:
- Violent crimes: These involve offenses such as assault and robbery, with rates showing consistent totals relative to state averages.

- Property crimes: This category encompasses burglary, theft, and vandalism, demonstrating a worrying upward trend recently.

- Quality-of-life offenses: Minor disturbances, loitering, and public intoxication incidents add to the cumulative perception of insecurity.

When comparing crime rates per capita, property crimes have emerged as the most frequent, exceeding city and state averages. Geographic distribution analyses indicate significant crime corridors and hot spots largely clustered around business districts and parks frequented by residents. Temporal patterns denote an increase in incidents during specific times, particularly between 10 PM and 2 AM on weekends, coinciding with nightlife activities.

Offender and victim profiling, while limited in detail, indicates that property crime victims often belong to lower-income households, while offenders may demonstrate recurring patterns of criminal behavior in the community.

Key issues identified within the locality encompass an increasing prevalence of property crimes, notably through car theft and break-ins, as well as emerging trends related to online scams and fraud.

Terrorism & Hate Crime Assessment

Historically, the area shows low incidence levels of terrorism or hate crimes. However, a comprehensive investigation into groups and actors reveals that certain extremist organizations have attempted recruitment efforts in the wider Los Angeles area, albeit with minimal impact locally. The Company HQ, due to its corporate nature, may present a symbolic target given its affiliation with a larger industry.

The current threat environment appears stable, although law enforcement agencies continue surveillance on neo-extremist activities influenced by national and international events. Recent alerts highlight the importance of remaining vigilant against ideologically motivated threats.

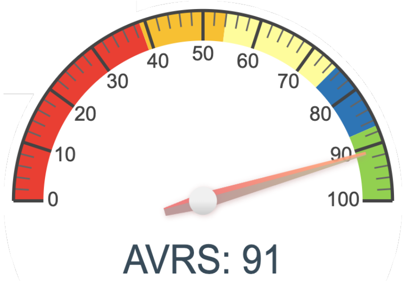
Civil Unrest & Social Risk

Historical data indicates sporadic unrest or protests concerning political or social movements, with recent tensions derived from nationwide trends concerning labor rights and social justice. The impact of these movements on safety and operations can be felt in heightened law enforcement presence and occasional disruptions.

In summary, while the overall crime environment remains manageable, continuous monitoring and analysis of emerging threats, particularly concerning property crime and socio-political tensions, are advised to ensure ongoing site security and community safety.

QUANTITATIVE RISK ANALYSIS

Asset Vulnerability Risk Score (AVRS)



The Asset Vulnerability Risk Score (AVRS) renders a quantitative numeric ranking on the scale of 1-100, based on vulnerabilities identified and the asset's unique environmental and circumstantial factors. The higher the score, the safer the asset is.

The AVRS provides a tool to compare diverse asset variants based on unique risks identified for each. Additionally, the tool facilitates understanding risk conditions, enabling objective cross-facility comparative analysis while incorporating structural, environmental, and circumstantial variables.

The AVRS incorporates documented vulnerabilities with the assessor's chosen risk level and mitigation priorities. Additionally, the numeric result considers each security layer's importance as it pertains to the overall protection of the asset and assessment of the environmental variables, including facility type, history, operations, and current threats in the context of the real-time environment.

Definitions

Minor Risk	**88-100**	**Based on analysis of the asset type, size, and sensitivity as it applies to both human and environmental threats, the asset is at minor risk, receiving a well above-average Asset Vulnerability Risk Score (AVRS). Few vulnerabilities were identified, which may require mitigation to enhance security.**
Low Risk	**76-87**	**Based on analysis of the asset type, size, and sensitivity as it applies to both human and environmental threats, the asset is at low risk, receiving a slightly above-average Asset Vulnerability Risk Score (AVRS). Some vulnerabilities were identified, which require immediate attention to enhance security.**

Medium/Average Risk	55-75	Based on analysis of the asset type, size, and sensitivity as it applies to both human and environmental threats, the asset is at medium risk, receiving an average Asset Vulnerability Risk Score (AVRS). Some significant vulnerabilities were identified, which require immediate attention to enhance security.
High Risk	40-54	Based on analysis of the asset type, size, and sensitivity as it applies to both human and environmental threats, the asset is at high risk, receiving a below-average Asset Vulnerability Risk Score (AVRS). Consequential vulnerabilities were identified in areas significant to asset security. Immediate collaborative efforts are required to improve the asset's security posture.
Critical Risk	0-39	Based on analysis of the asset type, size, and sensitivity as it applies to both human and environmental threats, the asset is at critical risk, receiving a well below-average Asset Vulnerability Risk Score (AVRS). Consequential vulnerabilities were identified in various areas significant to asset security. Urgent collaborative efforts are required to improve the asset's security posture.

RISK ANALYSIS AND PRIORITIZATION

The information in this section summarizes the risk level analysis determined for each vulnerability identified. The risk level was established based on professional experience and deep analysis of the threat vectors derived from the vulnerability identified, current intelligence and past incidents, probability of occurrence and the potential impact to facility structure, personnel, reputation, and operational sustainability if a vulnerability is exploited in full. Risk level definitions were set as follows:

Minor (M)
There is a very low probability of an incident occurring in which the identified vulnerability is exploited. While similar or comparable incidents may or may not have occurred in the past, there is no current evidence suggesting an imminent threat. If an incident were to take place, it may result in minor cost and/or damage to assets in addition to the possibility of minor injuries to persons, short-term operational interruption with no reputational damage.

Low (L)
There is a low probability of an incident occurring in which the identified vulnerability is exploited. Similar incidents may have occurred in the past, in the region, at comparable facility types, or at a facility with a similar vulnerability. If an incident were to take place, it may result in low cost and/or damage to assets in addition to the possibility of minor injuries to persons, short-term operational interruption with no reputational damage.

Medium (Md)
There is a moderate probability of an incident occurring in which the identified vulnerability is exploited. Similar incidents may have occurred in the past, in the region, at comparable facility types, or at a facility with a similar vulnerability. If an incident were to take place, it may result in moderate cost and/or damage to assets in addition to the possibility of severe injuries and/or loss of life, medium-term operational interruption with limited or temporary reputational damage.

High (H)
Based on threat analysis and intelligence, the probability of an incident occurring in which the identified vulnerability may be exploited is likely. Similar incidents have occurred in the recent past, in the region, at similar facility types, or at a facility with a comparable vulnerability. If an incident were to take place, it might result in significant cost and/or damage in addition to the

possibility of severe injuries and/or loss of life, long-term operational interruption with long-term significant reputational damage.

Critical (C)

Based on threat analysis and intelligence, the probability of an incident occurring in which the identified vulnerability is exploited is highly likely. Similar incidents have frequently occurred in the recent past, in the region, at similar facility types, or at a facility with a comparable vulnerability. If an incident were to take place, very significant cost and/or damage may be incurred in addition to the possibility of severe injuries and/or significant loss of life, permanent operational interruption, danger to organizational stability with long-term significant reputational damage.

Recommendations prioritizing mitigation were assigned to each vulnerability identified. Prioritization factors are based on risk severity, the assessed threat, the potential impact on the facility and personnel, the estimated resources available, and the urgency to take remedial action:

Accept (Ac)

Identified risks have been evaluated as acceptable or tolerable. No further remedial actions are required at this time. Re-evaluation is required periodically, or in the case new information becomes available.

Transfer (Tr)

Risk should be transferred to a third party, including but not limited to an insurance provider, release, waiver, or official documentation.

Mitigate C (MC)

The identified vulnerability and associated risk should be re-evaluated periodically. Remediation should take place in the foreseeable future, when time and/or resources become available.

Mitigate B (MB)

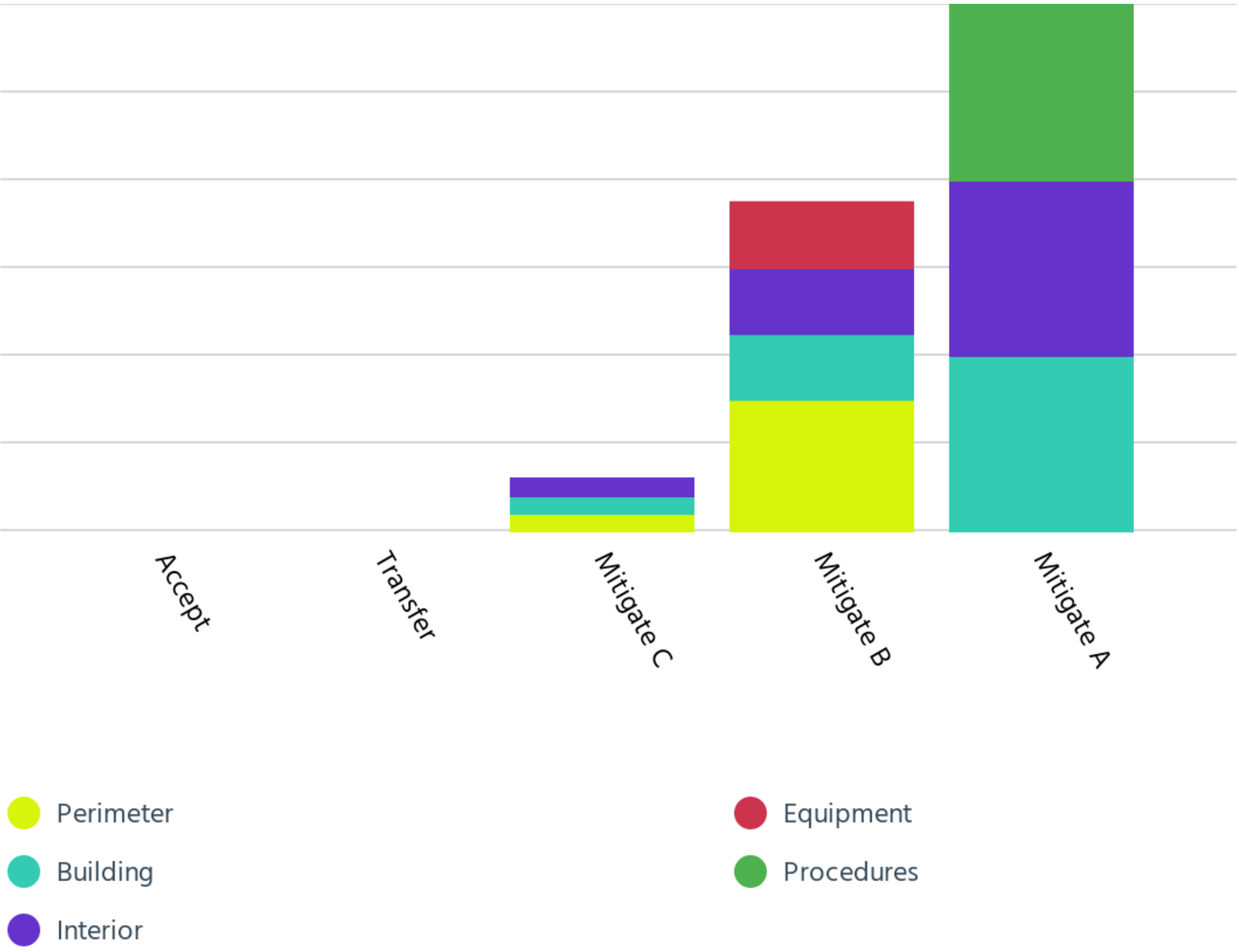
The identified vulnerability and associated risk should be remediated as soon as time and/or resources become available.

Mitigate A (MA)

The identified vulnerability and associated risk are of the highest priority and should be remediated immediately. Temporary solutions may be applied until the vulnerability and risk are sufficiently addressed.

RISK LEVEL	SECTION	AREA	VULNERABILITY	PRIORITY
High	Building	Emergency Exit	Rapid Egress Denial- Fire Hazard	Mitigate A
High	Interior	IT/Server Room	Insufficient Security Camera Coverage	Mitigate A
High	Procedures	Access Control	Insufficient Access Control Procedures	Mitigate A
Medium	Perimeter	Fence	Deficient Perimeter Fence/Wall	Mitigate B
Medium	Perimeter	Parking Lot	Insufficient Lighting	Mitigate B
Medium	Building	Building Frontage	Excessive Access Points	Mitigate B
Medium	Interior	Main Office	Insufficient Access Control	Mitigate B
Medium	Equipment	Video Assessment and Surveillance System (CCTV)	Outdated Security Camera System	Mitigate B
Low	Perimeter	Parking Lot	Vehicular Impact	Mitigate C
Low	Building	Building Frontage	Structural Weakness/Unprotected Glass	Mitigate C
Low	Interior	Main Office	Unprotected Glass	Mitigate C

Section by Mitigation Priority



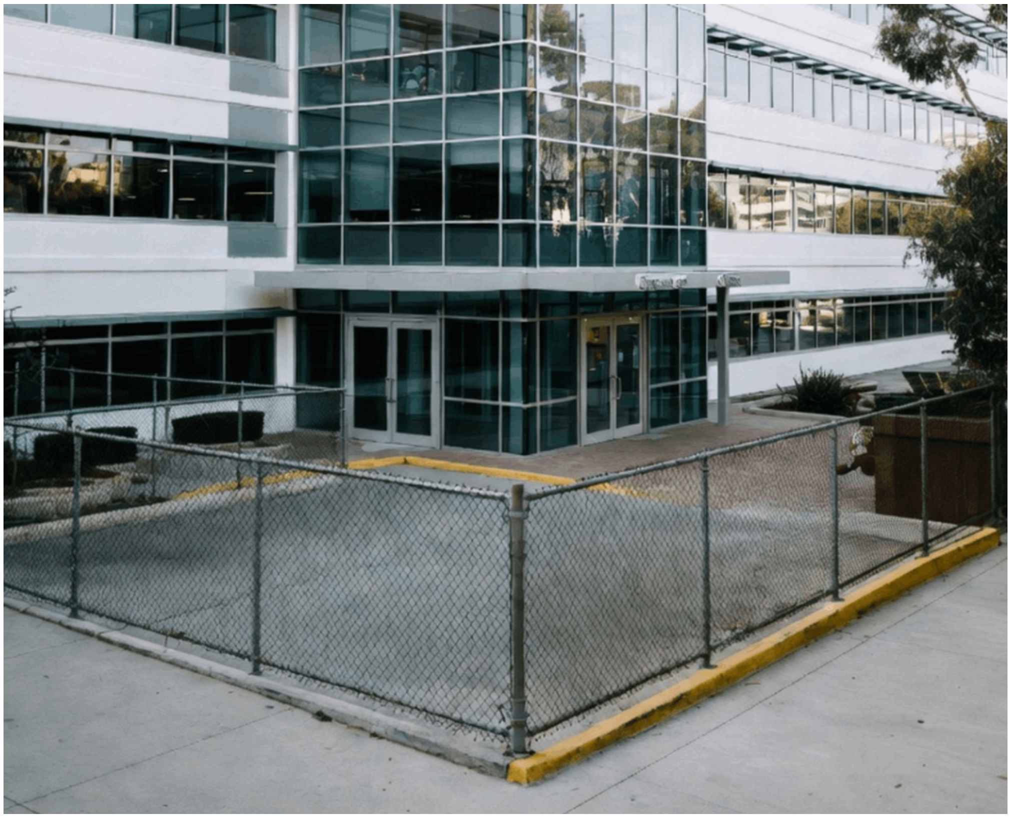
PERIMETER

Fence

MB Md

Vulnerability: Deficient Perimeter Fence/Wall

The facility is not enclosed within a perimeter boundary such as a fence or wall. The existing perimeter is insufficient and will not prevent an intruder from accessing exclusive areas.



Recommendations

- **Anti-Climb Fencing**

Install an anti-climb fence or wall. Different styles of anti-climb fencing are available, most consisting of vertical bars with horizontal supports designed to make scaling difficult. Additional measures may include appropriate lighting, security cameras, alarm devices, and signage to augment the perimeter boundary.

Reference: FEMA 426, 2-25

- **Fencing/Wall Enclosure**

Install a perimeter fence or wall enclosing the facility within a physical boundary. Fencing types include but are not limited to chain-link, aluminum, anti-climb (CPTED), barbed wire, concertina, triple-stranded concertina, welded mesh, buried fencing, wrought iron, and wire, all of which are designed to deter and delay intrusion. Additional measures may include appropriate lighting, security cameras, alarm devices, and signage to augment the perimeter boundary.

Reference: FEMA 426, 2-53

Parking Lot

MB Md

Vulnerability: Insufficient Lighting

There is insufficient lighting in the parking lot. Inadequate lighting creates general safety hazards and may promote unlawful activity in the area. Additionally, limited lighting may render existing surveillance equipment ineffective.

Recommendations

- **Illumination Quality Upgrade**

Upgrade the current parking lot light bulbs and/or luminaires for better illumination capabilities. Different light sources have different abilities and limitations. When choosing the optimum light source, various factors should be considered, such as the threat level, cost of change and usage, life usage expectancy (in hours), accessibility, maintenance, environment, and design

Reference: ASIS-Physical Security , P. 71, P.169-185

- **Standby Lighting**

Where continuous lighting is not required, install standby lighting within the parking lot. Standby lighting activates when motion is detected by the sensor.

Reference: FEMA 426, 2-68

MC L

Vulnerability: Vehicular Impact

Both the facility's exterior and pedestrians in the parking lot are vulnerable to vehicular impact. Injuries and/or structural damage may occur due to an accidental or intentional vehicular incident.

Recommendations

- **Planter Placement**

Place planters in strategic locations in and around the parking lot. Planters should be anchored and filled with weighted material to prevent displacement in the event of a collision. Ensure planters installed do not interfere with routine operations, visibility, or emergency response access.

Reference: FEMA 426, 2-45, B-21

- **Traffic Regulatory Signage**

Post regulatory traffic signage in and around the parking lot to remind drivers of traffic flow and vehicle speed regulations. Ensure crosswalks, waiting areas, and high-risk areas are appropriately marked to inform passing motorists.

Reference: FEMA 426, 2-70

- **Bollard Installation**

Install bollards along vulnerable areas in the parking lot. Bollard size and depth are determined by the vehicular threat level and should typically not exceed 30 inches in height. Bollard spacing should be between 36 to 48 inches (0.9 and 1.2 meters), comply with ADA regulations, and facilitate emergency response access.

Reference: FEMA 426, 1-41, 2-20, 2-37, 2-42

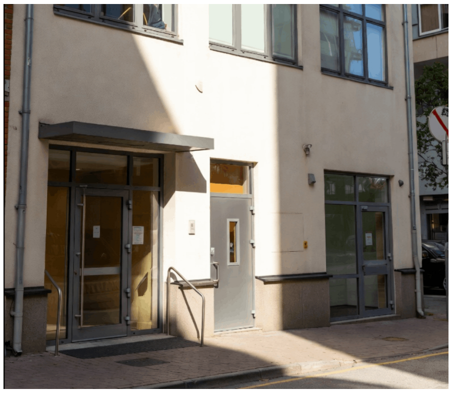
BUILDING

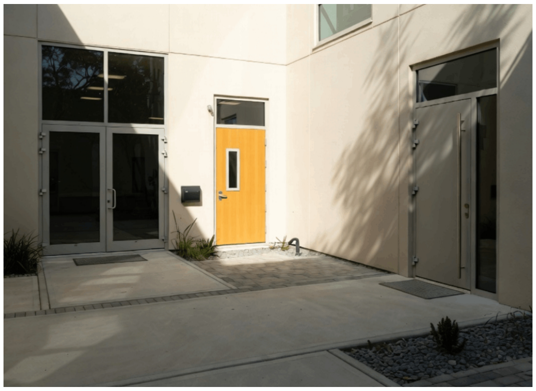
Building Frontage

MB Md

Vulnerability: Excessive Access Points

There are multiple access points along the building frontage providing access to the facility. An excess number of access points can make the facility more susceptible to unauthorized entry. Multiple access points are difficult to monitor and make proper access control challenging. Additionally, efforts to secure the facility in a lockdown may be delayed.





Recommendations

- **Access Point Minimization**

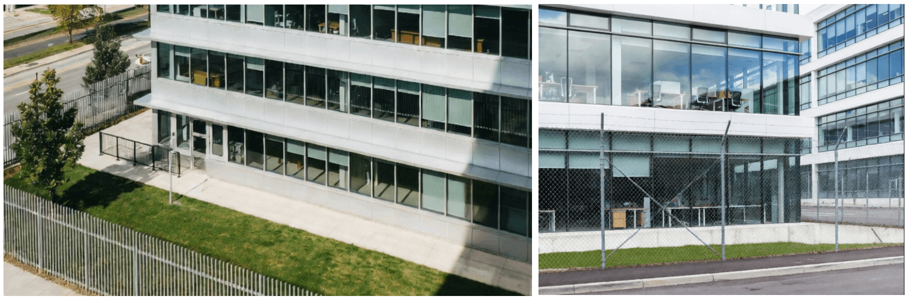
Depending on security resources available, access using entry points along the building frontage should be limited to one single entry point, where visitors can be screened appropriately before entering the facility. Alternate access points may serve as exits or entryways for credentialed staff and authorized personnel. Preferably, alternative entrance points should be equipped with remote monitoring, intrusion detection, and designed to prevent entry of unauthorized personnel.

Reference: FEMA 426, 1-40, APTA SS-SIS-S-010-13, Rev. 1, P.26

MC L

Vulnerability: Structural Weakness/Unprotected Glass

The material or design of the building frontage is not resilient and may be vulnerable to damage or intrusion. Materials such as unprotected glass and hollow wood increase the risk of potential intrusion, damage to the facility, or injury to personnel. In an explosion, lite materials such as glass and wood may be projected into the facility at high speed, resulting in injury or damage.



Recommendations

- **Glass Protection Film**

Treat the unprotected glass along the building frontage with shatter resistant, fragment retention, tinted and anchored protective security film. While the security film may limit glass fragmentation and delay an intrusion, the tinting will provide additional privacy screening so an aggressor cannot easily see inside the building.

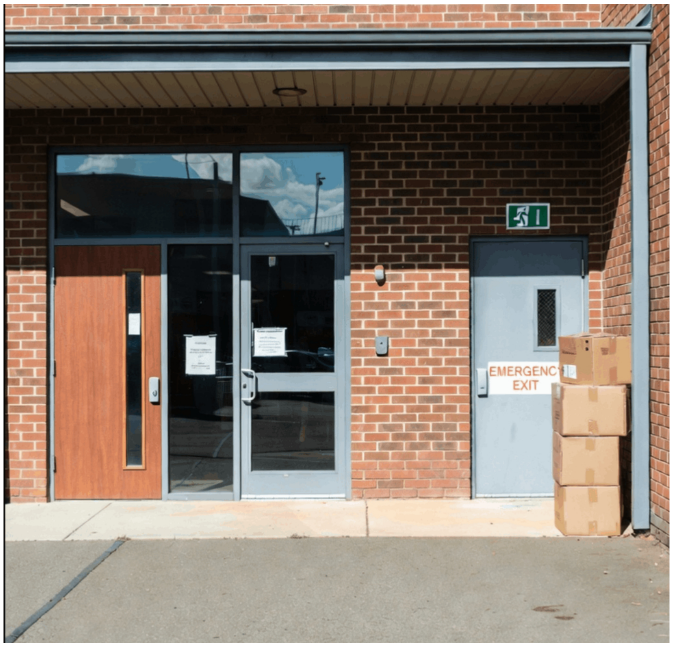
Reference: FEMA 426, 1-35, 3-73

Emergency Exit

MA H

Vulnerability: Rapid Egress Denial- Fire Hazard

The emergency exit door/gate may violate fire code, potentially restricting or delaying emergency egress of facility occupants. A malfunctioning lock, improperly installed locking device or blocked route may result in delayed and disorderly evacuation in case of an emergency.



Recommendations

- **Egress Pathway Clearance**

Ensure the area leading to and around the emergency exit is clear of debris and clutter to facilitate quick evacuation in case of an emergency.

Reference: NYPD Engineering Security Protective Design for High Risk Buildings, Pg. 62

- **Crash Bar Installation**

Install a crash bar on the emergency exit's interior, which quickly unlocks when pressure is applied in the direction of egress. Ensure a door spring is installed to prevent the door from remaining open after use.

Reference: FEMA 426, B-7

INTERIOR

Main Office

MB Md

Vulnerability: Insufficient Access Control

Access to the main office is not adequately controlled through one or more of its entrances. Facility equipment, property or personnel may be at risk. In the case of an incident, the ability to conduct a proper post-incident investigation is limited.

Recommendations

- **Locking Device Installation**

Ensure access to the main office is adequately controlled using a conventional lock, electronic or mechanical key code, RFID card reader/Fob or facial/biometric system to verify the authenticity of persons entering the area. For an office requiring elevated security measures, two-factor authentication access control may be considered. Distribute keys and/or RFID cards to authorized personnel, implementing proper documentation and tracking procedures. Avoid providing keys to vendors and ensure keys cannot be easily duplicated.

Reference: FEMA 426, 5-40

- **Vendor Escort Procedure**

Ensure vendors and maintenance personnel seeking access to the main office are accompanied and observed by authorized facility personnel throughout the duration of their required stay.

MC L

Vulnerability: Unprotected Glass

The main office design incorporates unprotected glass which may increase the risk of intrusion and limit the ability to thoroughly lockdown the room. In the case of an explosion, extreme weather, or seismic event, glass fragments may cause injury to personnel.

Recommendations

- **Glass Protection Film**

Treat unprotected glass in the main office with shatter resistant, fragment retention, anchored protective security film. Window tinting may be considered for added privacy.

Reference: FEMA 426, 1-35, 3-73

IT/Server Room

MA H

Vulnerability: Insufficient Security Camera Coverage

Activity in the IT/server room is not sufficiently monitored and/or documented by a security camera system. The ability to identify and track individuals accessing the room or respond to unlawful activity is limited and may be delayed, potentially exposing property and personnel to associated risks. Limited security cameras may encourage unlawful or unauthorized activity in unsupervised areas and hinder the ability to conduct a thorough post-incident investigation.

Recommendations

- **Security Camera Replacement**

Install security camera/s to monitor activity within the IT/server room. Adequate security camera coverage may substitute the need for frequent patrols to the area. Ensure camera placement facilitates the identification of all individuals entering or exiting the room. The camera type/model installed should function in all lighting conditions providing coverage of the entire room. For increased deterrence, install cameras in overt locations, strategically placed to avoid vandalism or sabotage. Motion sensors may also be used to detect movement in vulnerable areas and prioritize monitoring.

Reference: ASIS-Physical Security P.135, FEMA 426, 4-21, 5-44, NYPD Engineering Security Protective Design for High Risk Buildings, Pg. 54

EQUIPMENT

Video Assessment and Surveillance System (CCTV)

MB Md

Vulnerability: Outdated Security Camera System

The existing video assessment and surveillance system is outdated. The cameras render poor image quality, may not be IP accessible and have limited sensory and analysis capability. Although functional, the current system does not meet modern technological standards and offers limited surveillance capability. The use of outdated equipment provides a false sense of security and may require additional resources to ensure minimum security standards are met.

Recommendations

- **Security Camera System Upgrade**

Upgrade the facility's existing video surveillance system. Install surveillance cameras along the facility's perimeter, around access points, intakes and in areas where vehicles or pedestrians may approach the facility undetected. Ensure cameras are also installed to monitor activity indoors and in common areas. For maximum effectiveness, cameras should be monitored continuously and in real-time. Install most cameras in overt areas to maximize deterrence. Place cameras in locations with a sufficient view of the desired area where they are not vulnerable to vandalism, sabotage, or environmental damage. Ensure the new system is IP or network accessible. The installation of IP-based electronic security systems can be installed independently of major facility renovations.

Reference: FEMA 459, 5.10

PERSONNEL

Security Coordinator

Vulnerability: Undesignated Security Coordinator

The facility has not assigned a security coordinator to manage facility security needs with local law enforcement agencies, municipalities, or security vendors. Without a designated security coordinator, short and long term security-related matters may not be addressed, and organizational security-related interests may not be adequately achieved. A security vendor by itself cannot represent all the facility's security-related matters as vendors are likely to see only a partial picture of the organization's functionality. Without a security coordinator, proper tracking and supervision are unlikely to be accomplished.

Recommendations

- **Designated Security Coordinator**

Assign a security coordinator to manage and regulate the security needs and interests of the facility. Coordinator designation should be a staff member who can sufficiently address all relevant aspects and can track, supervise and execute security-related decisions. A security coordinator should usually be assigned even if the facility employs a security vendor as the primary security point of contact. Ensure the security coordinator has some relevant background and/or understanding of security and shares the understanding of security's importance. Ensure to send the security coordinator to relevant training.

PROCEDURES

Access Control

MA H

Vulnerability: Insufficient Access Control Procedures

The facility access control procedures are insufficient permitting unvetted visitors access to the facility. Areas with insufficient access control procedures (e.g., security screening, registration, and monitoring) expose facility personnel and assets to increased risk.

Recommendations

- **Visitor Management System**

Utilize a visitor management system as part of the facility's access control procedures. A visitor management system may expedite several access control processes to include efficient entry, vetting, issuing of guest badges, and record-keeping. The system may also enhance procedures such as sign-in, escort requirements and even mail review. Some systems even display limited "background check" data as an additional screening layer.

Reference: ASIS-Physical Security, P. 254

- **Approved Vendor List**

Create and maintain an approved vendor list for efficient vetting procedures upon arrival. In the list, include each vendor's complete information, including a photo. Run a periodic background check for each, including applicable watchlist databases. Establish each vendor's status, hours/days of operation to detect any unauthorized deviation from the pattern. Specific instructions defining security checks, such as mandatory escort requirements, should be established for each vendor.

- **Access Control Procedures**

Establish visitor access control procedures regulating and screening admittance to different areas of the facility, such as access gates, parking areas, offices, elevators, etc. Procedures should determine personnel responsible for general access to the facility (professional guard services, reception, staff, volunteers, etc.), the level of security screening (identification badges, registration requirements, etc.) and the security systems used (screening technologies, locking systems, access codes, visitor management, etc.). The access control procedures should define and address various visitor types (staff, students, vendors, VIP, etc.). Access control procedures are a vital component of the facility's security and a primary method to prevent, detect and deter potential aggressors.

Reference: FEMA 426, 4-14, 5-6

REFERENCES

1. *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings - FEMA-426/BIPS-06/October 2011, Edition 2*
2. *U.S. Department of Veterans Affairs, Physical Security and Resiliency Design Manual, October 1, 2020 , Revised May 1, 2024*
3. *Taking Shelter from the Storm: Building or Installing a Safe Room for Your Home, Includes Design Plans-FEMA P-320, December 2024, Sixth Edition*
4. *Guide for Developing High-Quality School Emergency Operations Plans - US Department of Education, June 2013*
5. *Safe Rooms for Tornadoes and Hurricanes-Guidance for Community and Residential Safe rooms- FEMA P-361, November 2024 Fifth Edition, Second Issuance*
6. *Physical Security for Public Transit - APTA Standards Development Program - Recommended Practice - American Public Transportation Association- SS-SIS-S-010-13, Rev. 1, May 23, 2023*
7. *Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings-FEMA-428/BIPS-07/January 2012, Edition 2*
8. *A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings FEMA 452 / January 2005*
9. *Incremental Protection for Existing Commercial Buildings from Terrorist Attack Providing Protection to People and Buildings- FEMA 459 / April 2008*

10. Manual of Security Policies and Procedures - US Department of Commerce -29-May-2017
11. New York Police Department, Engineering Security, Protective Design for High Risk Buildings - 2009 Edition
12. Design Guidance for Shelters and Safe Rooms- FEMA 453 / May 2006
13. DHS Bomb Threat Checklist- https://www.cisa.gov/resources-tools/resources/bomb-threat-checklist
14. Earthquake Safety Checklist- FEMA B-526 / October 2023
15. 2016 DHS-DOJ Bomb Threat Guidance Brochure - https://www.dhs.gov/sites/default/files/2024-12/24_1205_fps_bomb-threat-procedures-card-508.pdf
16. FEMA: Parent-Student Reunification Procedures (from Washington Military Department’s Emergency Management Division), April 2011
17. Fire/Emergency Medical Services Department Operational Considerations and Guide for Active Shooter and Mass Casualty Incidents, 2013
18. FEMA - IT Disaster Recovery Plan: https://www.ready.gov/business/emergency-plans/recovery-plan
19. FEMA: Developing and Maintaining Emergency Operations Plans, Comprehensive Preparedness Guide (CPG) 101, May 2025, Version 3.1
20. DHS:US Secret Service: Enhancing School Safety Using A Threat Assessment Model: An Operational Guide for Preventing Targeted School Violence , 2018, https://www.secretservice.gov/sites/default/files/reports/2020-10/USSS_NTAC_Enhancing_School_Safety_Guide.pdf
21. Severe Weather Planning for Schools, National Clearinghouse for Educational Facilities, 2008, https://files.eric.ed.gov/fulltext/ED539488.pdf
22. Design Guide for Improving Critical Facility Safety from Flooding and High Winds-FEMA 543 / January 2007
23. National Incident Management System (NIMS), Department of Homeland Security, December 2008
24. A Resource Guide to Improve Your Community’s Awareness and Reporting of Suspicious Activity/ FEMA P-904/ February 2012
25. ASIS International - Protection of Assets, Physical Security, 2012
26. Center For Disease Control and Prevention (CDC)- Coronavirus disease 2019- https://www.cdc.gov/coronavirus/2019-nCoV/index.html
27. World Health Organization - Novel-Coronavirus-2019- https://www.who.int/emergencies/diseases/novel-coronavirus-2019
28. US Department of Labor- Occupational Safety and Health Administration-OSHA 3990-03 2020