

Crime Impact Statement

Fire Station, Blackley



Figure 01 - Site Birds Eye View (Source: Google Maps)

Document Number: R022CIS-GS-SY-ZZ-RP-Y-0001-S4-A

Revision: A

Date of Issue: 13/02/2023

Status: Submitted for Review

Author: NH

Distribution: Steve Thomas

**Bradshaw Gass & Hope
LLP**

1 Executive Summary	2
2 Development & Surroundings	4
3 Development Layout & Uses	5
4 Crime Risk Assessment	7
5 Security Design Requirements	15
6 Security Requirements Statements	16
7 Recommendations – Building Operations	17
8 Recommendation – Physical Security	18
9 Recommendation – Access Control	20
10 Recommendation – Video Surveillance	24
11 Summary	25

1 Executive Summary

This report describes a Security Needs Assessment (SNA) completed by Graphite in support of the design and construction of a new Fire Station at Rochdale Rd, Manchester M9 7EQ, United Kingdom.

This development has been assessed using the principles of 'Crime Prevention Through Environmental Design' (CPTED) in order to identify any opportunities for crime and the fear of crime.

Please note: Greater Manchester City Council may recommend that a planning condition is added that reflects the physical security section of this report.

The CIS considers security threats to the proposed development and security vulnerabilities apparent in the architectural designs and proposed use. The CIS follows a security design methodology to provide security recommendations that should be designed and specified in future project stages. These recommendations are specifically intended to mitigate security risks to the development, its users and the surrounding area.

1.1 Security Recommendations

This CIS report provides a suite of security risk mitigation options for consideration. These recommendations aim to mitigate the security risks to the development in a pragmatic and proportionate manner while considering their potential impact on the proposed budget, operation and appearance of the building.

Comments on the security recommendations in this report are invited from the client and design team, in order to ensure compatibility with the operation, design and budget.

2 Development & Surroundings

2.1 Visual Audit



Figure 02 - Site Plan (Source: Google Maps)

The site is located within Manchester City Council, as this is an existing Fire Station the development fits in perfectly. The site is surrounded by Rochdale Road (west), White Moss Road (south), Levedale Road (north) and Elmton Road (east). The development is surrounded mostly by residential use types, places of worship and commercial units.

2.2 Site Survey



3 Development Layout & Uses

3.1 Site Plan



Figure 03 - Site Plan (Source: Bradshaw Gass & Hope LLP)

The site will consist of a singular building, training yard, training tower and sufficient amount of parking. The front of the site is not to be boarded off with fencing like most Fire stations as fast and quick access is required. A secure line is still created along the building facade creating a secure rear yard of the Station.

4 Crime Risk Assessment

Graphite Security uses police crime statistics to support our assessments of crime risks. Police statistics consider the development site to be within the Charlestown 'policing neighbourhood' within the Greater Manchester Police Police Service force area.

Warning: Crime Data Missing

Due to an IT systems problem at **Greater Manchester Police**, data for crime may be missing from July 2019 onwards. The force is working to rectify this issue. In the meantime, you can check previous months using the dropdown boxes below, which will allow you to judge historical crime levels.

Due to the **lack of crime recordings** from Greater Manchester Police, we have taken the historical crime statistics available from 2018 to 2019 and little to nothing from 2020-22.

4.1 Charlestown

<https://www.police.uk/pu/your-area/greater-manchester-police/charlestown/?tab=statistics>

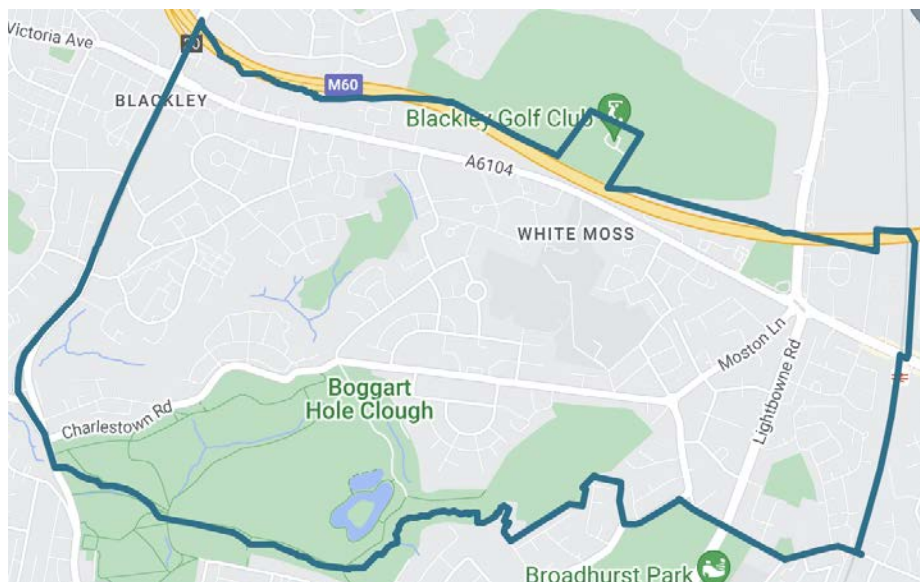


Figure 04 - Charlestown 'Policing Neighbourhood'

Information is accessible on www.police.uk reveals that crime and disorder in that area within the years 2020 to 2022 was dominated by:

- Anti-social Behaviour

	ASB	Burglary	Robbery	Vehicle	Violent	Shoplifting	CD&A	Other Theft	Drugs	Bike Theft	Theft From the Person	Weapons	Public Order	Other	Total
Jun 2019	31	7	4	7	95	12	18	32	37	1	75	6	25	6	356
May 2019	25	5	2	10	58	7	24	9	3	1	1	3	29	4	181
Apr 2019	37	11	4	9	71	7	15	17	3	1	0	3	31	5	214
Mar 2019	49	17	3	15	73	2	28	7	2	1	6	2	37	2	244
Feb 2019	35	6	5	12	38	6	26	14	2	1	2	3	25	3	178
Jan 2019	36	10	4	11	47	5	13	8	0	0	0	4	23	3	164
Dec 2018	33	8	1	8	43	3	18	6	3	0	1	1	16	5	146
Nov 2018	28	6	2	10	42	4	23	15	2	0	0	5	21	4	162
Oct 2018	30	8	2	8	45	7	12	9	5	2	1	0	16	2	147
Sep 2018	31	5	5	5	45	5	20	7	4	0	0	6	18	5	156
Aug 2018	26	6	7	16	49	3	16	6	2	1	1	0	30	4	167
Jul 2018	31	8	10	9	64	5	32	5	2	0	0	4	36	1	207
Jun 2018	44	13	7	7	84	7	31	30	47	2	50	4	41	7	374
May 2018	42	11	2	9	64	4	18	8	0	0	3	0	30	2	193
Apr 2018	48	7	4	16	35	4	22	5	2	2	2	2	25	9	183
Mar 2018	26	15	2	11	55	3	13	12	2	0	2	0	23	5	169

Figure 05 - All crime types in Higher Blackley between March 2018 to June 2019.

The crime rate peaked in June 2018 dominated by violent crime type. The lowest recorded crime recorded was in December 2018 dominated by violent crime type.

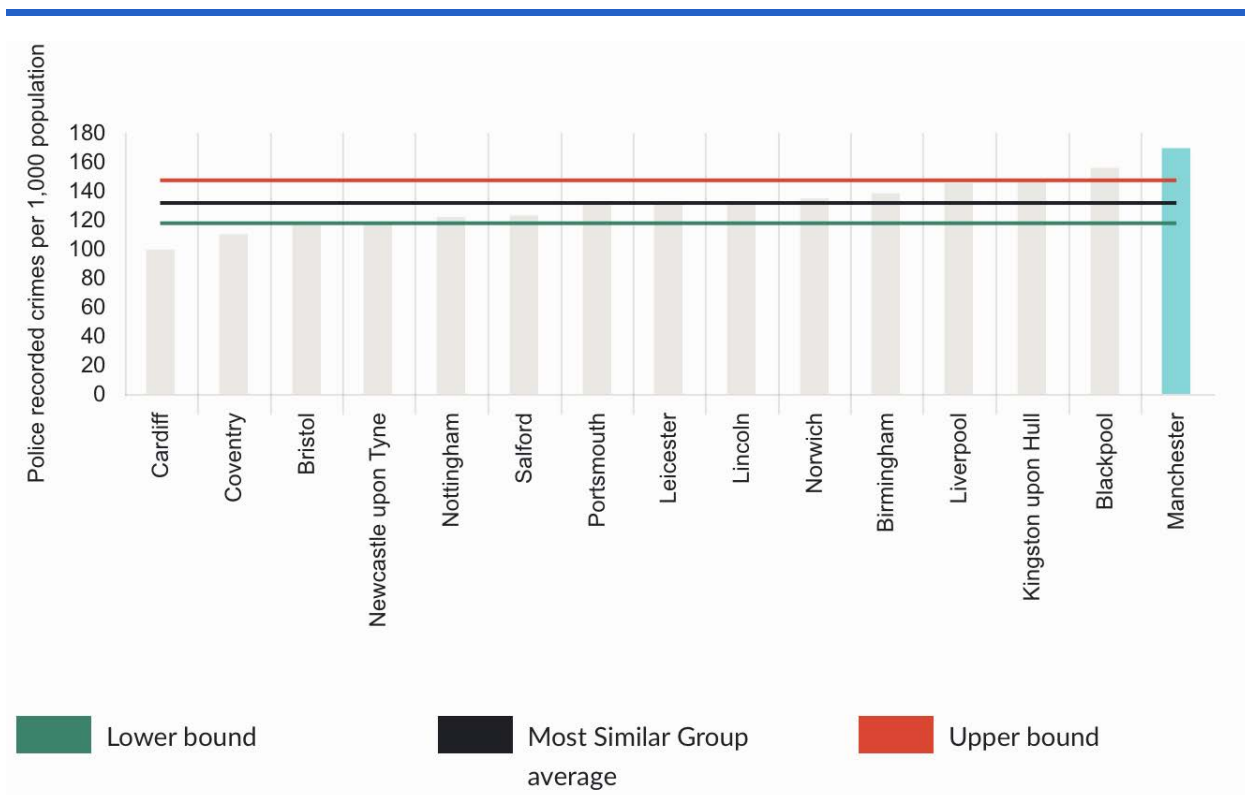


Figure 06 - Crime in Manchester compared with crime in similar areas (ending in March 2022).

In the year ending March 2022, the crime rate in Manchester was higher than the average crime rate across similar areas.

This chart compares the crime rate in your local area to the average crime rate across similar areas. It shows the total number of crimes over a twelve-month period per thousand residents, for the crime type selected. The red and green lines show how far the crime rate would normally vary from the average. Manchester lies above the red and green lines, so its crime rate is the highest for the group.

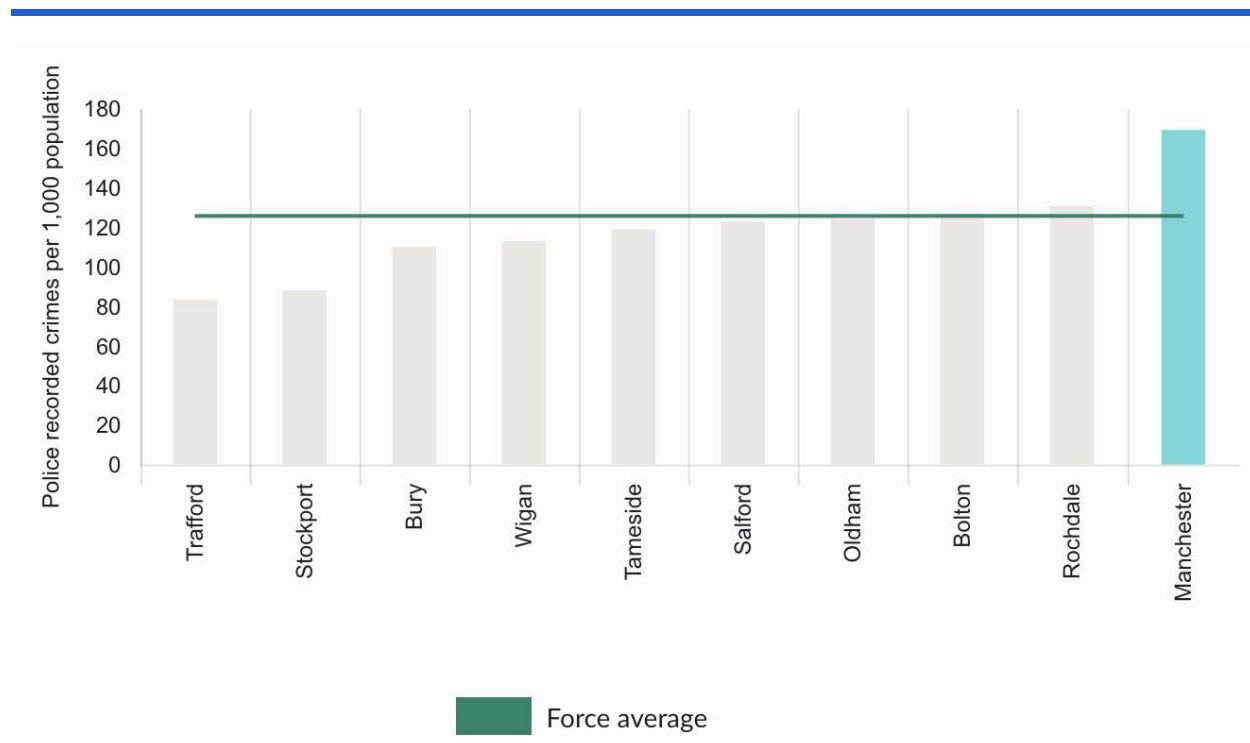


Figure 07 - Crime Stats of Manchester area compared to Greater Manchester Force Area (ending in March 2022).

The force's average crime rate is 125.85 and the Manchester area is 169.37 showing it is higher than the Greater Manchester force average.

The above figure shows all areas within the Greater Manchester Force Area comparing it to the force average crime rate, as you can see Manchester, where the development is situated is located towards the high end of the chart, with Manchester being the highest rated area.



Figure 08 - Crime changes over time in Manchester and in the Greater Manchester force area.

This chart shows how crime rates in your local area and police force area have changed over time. It also shows how the average crime rates in similar areas to the Manchester area have changed over time.

Threat Actors	Description	Reasonable Worst-Case Scenario
Threat - Opportunist Theft	Opportunist theft affects local community properties where a criminal in a legitimate location (e.g. Reception or Car Park) can readily observe a security vulnerability. Anecdotally, including police crime reporting, most opportunistic theft involving intrusion occurs through doors that have been left open, unlocked or unattended. The capability of opportunist thieves is also typically considered to be low, as they are unwilling to carry tools that could be considered as 'going equipped'.	A single threat actor attempts to breach the building envelope through open or unlocked doors or windows. Novice attackers with no tools. Covert.
Threat - Deception Theft	Similarly to opportunist theft, the use of deception to enter a premises is often seen as a lower risk on the part of the criminal. Commonly reported examples include criminals posing as services engineers or the authorities to convince staff to allow them access to a property, or a wide range of deceptions in order to effect the opening of a door to enable a violent entry.	A single threat actor attempts to breach the building by posing as a service engineer or the authorities to convince staff to allow them access to a property. Not categorised overt or covert.
Threat - Targeted Theft	Local community properties can be targeted by professional organised criminals for intrusion and theft if they are perceived to contain high-value portable items such as expensive equipment and personal goods.	Multiple threat actors attempt to breach the building envelope and internal security features using a range of hand tools. Overt. Experienced and knowledgeable attackers, using concealable hand tools and electronic devices. Covert.

4.2 Security Threat Categories

The table below categorises the previously discussed threats based on capability and intent, i.e. the number of attackers, their level of expertise and fitness, willingness to be caught or harmed and the tools and weapons available to them.

The table below combines similar threat actors into the same attack category, to provide a summary of potential 'reasonable worst-case' threats.

Attack Category	Reasonable Worst-Case Threat
Opportunistic Theft	A single threat actor attempts to breach the building envelope through open or unlocked doors or windows. Novice attackers with no tools. Covert.
Vandalism	A single or multiple actors deliberately destroying of or damage to public or private property. Novice attackers with improvised tools. Overt.
Anti-social Behaviour	Multiple actors causing harassment, alarm, or distress to a community, public spaces, or buildings. Novice attackers with no tools. Overt.
Targeted Theft	Multiple threat actors attempt to breach the building envelope and internal security features using a range of hand tools. Overt. Experienced and knowledgeable attackers, using concealable hand tools and electronic devices. Covert.
Mob Attack	Multiple threat actors attempt to damage the building and to breach the building envelope. Novice attackers with improvised tools. Overt.

4.3 Layering Security Measures

The effectiveness of security risk mitigation measures in combination is typically considered using a layered, or onion skin model comprising:

- Electronic security measures including intruder detection, video surveillance, and access control to provide to alert responders to threats
- Physical security measures including fences, vehicle barriers, walls, doors, and safes to deny or delay threat actors reaching their targets
- Operational security measures including procedures, risk assessment, monitoring, patrolling, and response.

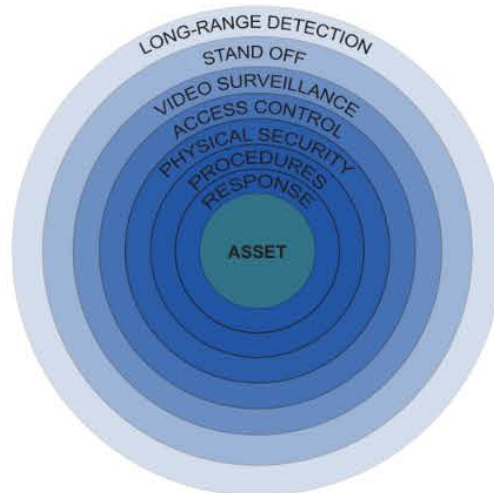


Figure 09 - 'Onion Ring' Model

In an urban setting, these layers are typically represented by:

- External Intrusion Detection Systems
- Boundary treatments and landscaping
- Video Surveillance
- Doors and Windows
- Internal Intruder Detection Systems
- Hold-up Alarm Systems (panic buttons)
- Refuge Areas
- Security guards, third-party security or police response

5 Security Design Requirements

7.1 Design Basis Threats

Based upon the threat categories highlighted earlier, the following table focuses on the 'reasonable worst-case' attack types that are proposed for specifying security measures. These are used as the 'design basis threats' (DBTs) for the specification of security measures.

7.2 Site-specific DBT's

Attack Category	Description
Experienced forced entry using manual attack	Two experienced aggressors using concealable hand tools to attempt entry into the building. The attack may generate some noise but will be intended as surreptitious.
Covert entry using technical attack	Two technically competent intruders using sophisticated tools and methods to attempt entry into the buildings. The attack may generate some noise but will be intended as surreptitious.

6 Security Requirements Statements

The Security Requirements Statement:

1. Categorises the various influencing factors into clear statements that can be addressed through security design and operating procedures
2. Ensures that security needs and project constraints are understood before security solutions are considered
3. Forms the basis for the specification of security measures and is referred back to during design development

This statement is intended as a succinct summary of the security requirements for the property.

It forms the basis of subsequent security recommendations and, once approved, should be referred back to during design and construction.

Site-Specific Security Requirements Statement

The security requirements for the development are:

- To provide security features that support the marketing and operation of the development through meeting or exceeding likely guest requirements.
- To provide security that is visible and reassuring without being imposing.
- To provide a safe and secure environment for staff, guests, and assets so that the security risk to them is 'as low as reasonably practicable based on 'reasonable worst-case' security threats.
- To facilitate the management as a controlled environment, with only authorised people being granted access beyond semi-public areas.
- To provide a robust property boundary and building envelope that will deter and delay threat actors from entering the site, harming the occupants, or removing property.
- To provide the above against the following Design Basis Threat:
 - Multiple experienced aggressors
 - Concealable hand tools

7 Recommendations – Building Operations

7.1 Crime Prevention Through Environmental Design

Recommendations are included below for consideration in the design of the development, based on the established principles of Crime Prevention through Environmental Design (CPTED); natural surveillance, natural access control, territorial reinforcement, maintenance and activity support.

Recommendations	Function
Provide suitable illumination to accessible areas around the buildings, including public open areas, all pedestrian routes, service roads and undercrofts.	To provide even illumination, and good colour rendition, during hours of darkness.
Provide lighting to all parking areas in accordance with BS EN 5489, with an average lux level of 20.	To provide illumination to parking areas during hours of darkness.
Provide suitable illumination to service areas in and around the buildings.	To provide even illumination, and good colour rendition, during hours of darkness.
Provide (PIR) detector-activated lighting to recesses and doorways.	To provide illumination when a person enters a recess.
Maintain shrub planting so that it does not exceed 1000mm in height. Maintain tree canopies so that they fall no lower than 2000mm from the ground.	To ensure clear sightlines.

8 Recommendation – Physical Security

8.1 Physical Security - Boundary Treatment

Recommendations	Function
Provide a secure boundary treatment to the rear yard with a height of at least 1.8m	To provide a secure boundary treatment to the site creating a secure fence line and reduce the chances of intrusion.

8.2 Physical Security - Site Access

Recommendations	Function
Provide vehicle entrance and egress points with gates matching the boundary treatment.	To restrict vehicle access to building users and authorised third-party vehicles e.g. delivery vans, waste collection and visitors.
Provide pedestrian entrance and egress points with gates matching the boundary treatment.	To restrict pedestrian access to building users and authorised third parties.

8.3 Physical Security - Glazing

Recommendations	Function
Provide laminated glass to accessible glazed areas. If compatible with the selected glazing system, use glass rated P1A or above under BS EN 356. If this is not possible, glazing should incorporate a PVB interlayer of a minimum thickness of 0.76 mm.	To provide glazing with a degree of resistance to physical attack. P1A is the lowest rating of manual attack resistance under the BS EN 356 standard. P1A glazing is typically around 6.8mm of glass and PVB interlayer.

8.4 Physical Security - Sectional Doors & External Doors

Recommendations	Function
Provide Sectional Doors of sufficient strength so the doors will deter and/or delay forced entry by the use of small portable hand tools (LPS 1175 SR2 or STS 202 Burglary Resistance 2 if possible).	LPS 1175 SR2 products provide resistance to opportunist attempts at forced entry, using bodily physical force and a range of hand tools, including those that create noise.
Provide back-of-house external doors, e.g. the delivery and dispatch area and fire exits, with doorsets certified to BS PAS 24 tested and certified.	To provide a resistance time of 3 minutes against a low-level set of tools.

8.5 Physical Security - Cycle Storage

To reduce the risk of theft of bicycles from bike storage areas, provide suitably robust furniture for staff and visitors to lock their bikes.

Recommendations	Function
Provide cycle racks, hoops or similar of robust construction securely fixed to the ground, floor or walls.	To provide a secure location for cycle storage.

9 Recommendation – Access Control

9.1 Access Control - Fire Station

To facilitate legitimate access to and within the station and to reduce the risk of intrusion occurring through deception, tailgating etc a layered access control system should be provided.

9.2 Access Control - Building Envelope and External

Recommendations	Function
Provide access control and intercom at the main entrance door.	To allow management of access via the main entrance.
Provide access control and intercom at the entrance doors to back-of-house areas, e.g. Staff Entrance.	To allow management of Staff access during and outside of working hours.

9.3 Access Control - Front of House Areas

We suggest that the following provision will mitigate the identified security risks, satisfy likely guest expectations and support the management of the station.

Recommendations	Function
Provide access control on doors leading from the secure Entrance Lobby and Community Room to Client operational areas. Ensure also that stairs are only accessible from the secured operational side.	To limit the ability of persons without appropriate access rights to gain access to operational areas.

9.4 Access Control - Back of House Areas

We recommend that the following provision would mitigate security risks and support building management.

Recommendations	Function
Provide access control to doors into offices containing sensitive information or high-value equipment.	To limit the ability of people to enter sensitive areas without appropriate Staff access tokens.
Provide access control to critical plant spaces.	To limit the ability of people to enter sensitive areas without appropriate Staff access tokens.

10 Recommendation – Video Surveillance

To deter crime and support the investigation of incidents in and around the development, the provision of a video surveillance system is recommended.

Cameras should be located, specified and coordinated to provide the required views, with an image resolution appropriate to the task and other performance factors such as low light performance specified to match the location and intended use.

We suggest that the industry-standard 30 days of recording time is provided for each camera in order to support post-incident investigations and to meet public expectations.

Recommendations	Function
Provide fixed external cameras to provide coverage of the main entrance and other building entrance points and refuse area/access route	To provide a view of a person entering the building.
Provide fixed external cameras viewing the pedestrian access routes to the site via external amenity spaces, service roads and streets.	To provide a view of vehicles and pedestrians entering the site.
Provide fixed camera(s) to provide coverage of the cycle parking area.	To provide a view of locked-up cycles.

11 Summary

It is concluded that security provision across all areas is proportionate to the risk with the levels of protection afforded through the physical protection elements. The additional layers of protection already within the security strategy can only serve to reinforce the physical security approach at this particular location.

This report has been produced based on all information collated, including but not restricted to, site drawing plans and associated documents, site survey, environmental visual audit, and by subsequent correspondence. Should any amendment to the design or build specification be necessary, I should be notified in order that this security assessment can be modified as required.

A handwritten signature in black ink, appearing to read 'Nasr Haque', written in a cursive style.

Nasr Haque