Crime Impact Statement
Avenue Road, London

Figure 01 - Proposed Context Massing (Source: Domvs London)

Document Number:	CIS03-GS-SY-ZZ-RP-Y-0001-S4-A	
Revision:	B	
Date of Issue:	13/04/2021	
Status:	Issued for Planning Use	
Author:	NH	
Distribution	Max O'Brien	Domvs London (Global Holdings) Ltd
	Greg Turner	Domvs London (Global Holdings) Ltd

Graphite Security

1 Executive Summary

This report describes a Crime Impact Statement (CIS) completed by Graphite Security in support of the design and construction of the proposed 12 x townhouses including communal Health and Wellness Spa at 52 Avenue Road, St Johns Wood, London, NW8 6HS.

'Demolition of existing building and erection of 3 blocks to provide 12 residential units (C3)'.

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: London Borough of Camden 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 operation, design and budget.

2 Tenant Security Provision

Recommendations in this report include provisions for the security and convenience of building tenants and their fit-out, e.g. facilitating ease of installation of security systems. However, the decision on whether and what security systems to provide within a tenant's demise is theirs and is outside of the scope of this report.

Electronic security measures within each tenants' demise are assumed to be provided by those tenants subject to their own security risk assessment and operational requirements.

Physical security measures to the perimeter of each tenants' demise are recommended in this report, based on our assessment of threats and vulnerabilities at the design stage. This does not preclude tenants from making their own security risk assessment and providing further enhancements.

Recommended security provision included within this assessment is based on a fit-out that offers full protection (within what would be termed a turn-key standard).

It is likely provision will be to the minimum standard to allow for the future tenant to complete a risk commensurate installation. This (minimum) Category A fit-out will negate some security provisions as listed below.

The SQSS has however ensured that items to promote future fit-out have been included as part of the initial build phase (ducting, pre-wiring etc. as required).

3 Development & Surroundings

3.1 Visual Audit

Figure 02 - Location Plan (Source: Google Maps)

The site is located within the London Borough of Camden and is approximately 1.4 miles from Camden City Centre and 0.5 miles from Primrose Hill high street.

The site is surrounded by high-end residential dwellings making the current development relevant and just. Primrose Hill Park is within very close proximity located to the east of the site.

4 Site Survey

Figure 03 - Site Visit Diagram (Source: Graphite Security Ltd)

5 Development Layout & Uses

5.1 Proposed Site Plan

Figure 04 - Proposed Site Plan (Source: Domvs London)

The plot is to be accessed from Avenue Road by a gated entrance and egress creating a secure one-way system. A third entrance is located off Elsworthy Road which is to remain closed at all times.

The development will provide 12 new townhouses including communal Health and Wellness Spa, each townhouse will provide sufficient car park spaces and a communal garden. The Health and Wellness Spa will be located at the basement level.

6 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 Swiss Cottage 'policing neighbourhood' within the Metropolitan Police Service force area.

6.1 Swiss Cottage

https://www.police.uk/pu/your-area/metropolitan-police-service/swiss-cottage/

Figure 05 - Swiss Cottage 'Policing Neighbourhood'

Information is accessible on www.police.uk reveals that crime and disorder in that area within the year 2020 to 2021 was dominated by:

- Anti-social Behaviour
- Violence and Sexual Offences
- Vehicle Crime
- Other Crime

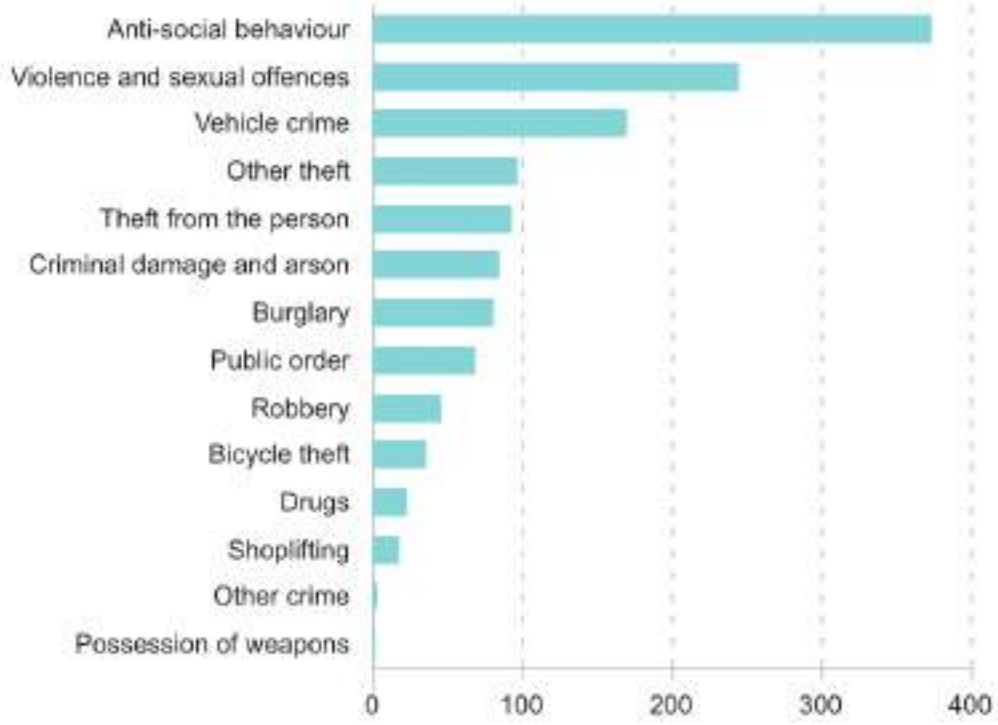

Figure 06 - All crime types in Swiss Cottage between Oct 2020 to Sep 2021.

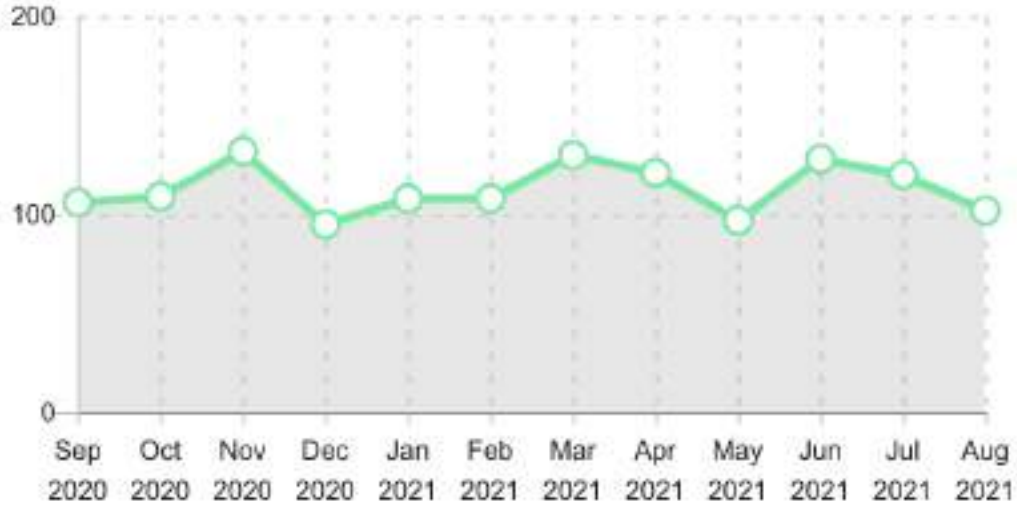

Figure 07 - All crime levels in Swiss Cottage between Oct 2020 to Sep 2021.

The crime rate peaked in November 2020 dominated by anti-social behaviour and violence and sexual offences. The lowest recorded crime recorded was in December 2020 dominated by anti-social behaviour and violence and sexual offences.

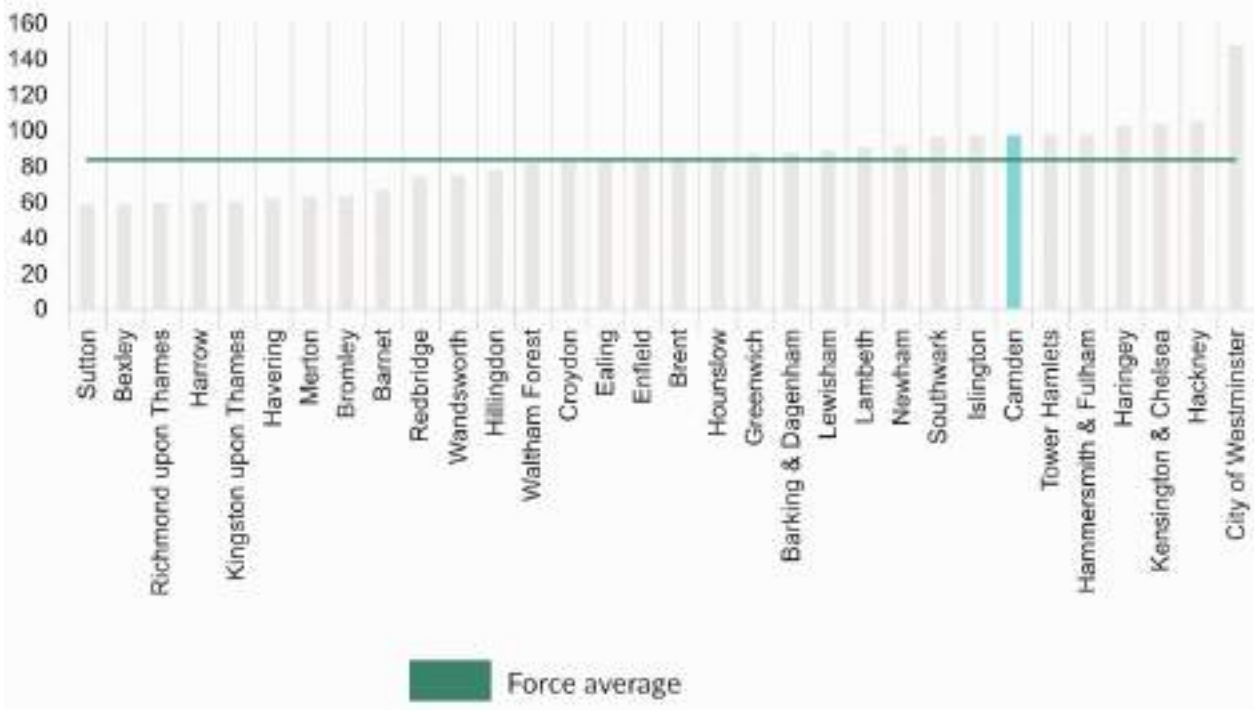

Figure 08 - Crime Stats of all areas in the Metropolitan Force Area (ending in March 2021).

The force's average crime rate is 83.41 and the Camden area is 96.93 showing it well above the Metropolitan force average.

The above figure shows all areas within the Metropolitan Force Area comparing it to the force average crime rate, as you can see Camden, where the development is situated is located towards the higher end of the chart, Camden being the 7th highest rated area.

Threat Actors	Description	Reasonable Worst-Case Scenario
Threat - Opportunist Theft	Opportunist theft affects residential properties where a criminal in a legitimate location (e.g. Public Pathway or Public Parking) 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 as overt or covert.
Threat - Targeted Theft	Residential properties can be targeted by professional organised criminals for intrusion and theft if they are perceived to contain high-value portable items such as cash, jewellery, computers, mobile phones and expensive clothing.	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.

6.2 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.

6.3 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 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

7 Security Design Requirements

7.1 Design Basis Threats (DBT)

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
Opportunistic theft: Opportunistic entry without physical force or violence.	A single threat actor attempts to gain illicit access to the building without forced entry or violence. The attacker will not carry significant tools or use techniques that make noise.
Targeted theft: Experienced forced entry using tools and/or violence.	Two experienced aggressors using concealable hand tools to attempt entry into the building. The attackers will be willing to generate noise. Examples could include forced entry via a rear door in order to access the dwelling.

8 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.

8.1 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:

□ Opportunistic entry and theft
□ Experienced Forced entry using manual attack

9 Security Management and Control

A dedicated location should be provided on-site to allow the building management team to manage the site and vehicle access, to monitor the site's video surveillance and intruder alarms and to coordinate an emergency response.

Recommendations	Function
Provide a security monitoring and control location within the site. This need not be a dedicated Security Control Room, a suitably located and equipped building management room may suffice.	To allow for the monitoring and management of security systems from the site.
Provide (where applicable) security monitoring and control location with an intercom connected to the building vehicle barriers.	To allow for the management of site vehicle access by the building management team.
Provide the security monitoring and control location with head-end equipment for access control, intercom, intruder alarms and video surveillance.	To allow for the monitoring and management of security systems.

10 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, and service roads.	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 detector-activated lighting to recesses and doorways.	To provide illumination when a person enters a recess.
Provide security signage at entrance points. Consider signage describing video surveillance (required by legislation) and security patrols.	To clearly indicate the security measures in place around and within the development.
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.

11 Vehicle Control and Hostile Vehicle Mitigation

To support the controlled operation of the site and to reduce the attractiveness of both public areas and buildings to a range of threats, we recommend that vehicle barriers and control measures are put in place.

Recommendations	Function
Provide building vehicle entrance and egress points with operable vehicle control measures, e.g. powered gates.	To restrict pedestrian and vehicle access to building users and authorised third party vehicles e.g. delivery vans, waste collection and visitors.

12 External 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 viewing residential entrances.	To provide a view of a person entering each building.
Provide fixed external cameras viewing the pedestrian access routes to the site via external amenity spaces.	To provide a view of vehicles and pedestrians entering the site.
Provide fixed external cameras viewing all designated parking spaces.	To provide a view of parked vehicles.

13 Recommendation - Physical Security

13.1 Physical Security - Boundary Treatment

Recommendations	Function
Provide a boundary treatment to the site with a minimum height of 1.8m.	To provide a secure boundary treatment to the site creating a secure fence line and reducing the chances of intrusion.

13.2 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.

13.3 Physical Security - External Doors

Recommendations	Function
Provide residential apartment entrance doors with BS PAS 24 tested and certified doors.	To provide a resistance time of 3 minutes against a low-level set of tools.

14 Recommendations - Intruder Alarm

14.1 Intruder and Hold-Up Alarm

The provision of any intruder and hold-up alarm to the residential dwellings will be the responsibility of the tenants. The recommendations below are intended to assist those tenants in installing appropriate equipment and to support the client in attracting security-conscious tenants.

Recommendations	Function
Consider providing an allocated space for an intruder alarm panel in each townhouse. Consider providing an allocated unswitched fused spur adjacent to the panel location.	To allow tenants to install an intruder alarm system with minimum disruption.

15 Recommendation - Access Control

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

Recommendations	Function
Provide building vehicle entrance and egress points with intercom and access control system.	To allow management of access to the site.
Provide access control to doors into back of house areas, e.g. Refuse and Bicycle Store. (If applicable).	To allow management of back of house access.

14 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.

With the above included, I am able to confirm that the above Crime Impact Statement is sufficient to satisfy the planning requirement.

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 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.

Nasr Haque