NaCTSO
National Counter Terrorism Security Office

ASSOCIATION OF CHIEF POLICE OFFICERS

Date: 2nd July 2014

# Guidance Note 1/2014

# Street View Imagery/3D Imagery Mapping

## Introduction.

This guidance note has been written in response to requests from business and industry following approaches from Street View Imagery/3D Imagery companies to photograph and map the internal footprints of publicly accessible sites.

This advice is **not** written to discourage use of imagery, but to provide some consideration of the security implications and value that this tool could provide to a person with criminal intent.

Corporate and personnel digital footprints can allow a person with hostile intent to obtain significant information that may assist in preparing an attack, whether that is Terrorism or Criminal related. The accessibility of publicly available internal imagery could add to attack planning capability if reasonable mitigation measures are not considered or implemented.

## Mitigation Considerations.

Prior to any attendance at the site by the imagery company to conduct photography, and having conducted due diligence checks on the company, a site should consider having some or all of the following measures agreed within the contract:

1. Agreement that all static and un-domed CCTV cameras be pixilated out of the Image. (This withdraws the ability to determine CCTV type or direction)

2. Agreement that all public/back of house access control measures be pixilated. This should include any electrical or mechanical measure and must include any external access control measure to car parks or delivery entrances. If a site has installed PAS 68 rated HVM measures these should **not** be pixilated as they will add to the visible robustness

of the site **but** the electrical and mechanical measures associated with them should be obscured.

3. Agreement that the time of the photography is determined by the site owner. The site owner should consider that the best time to have their site photographed would be during quieter periods of the site operation. This would deny a hostile the option of determining potential casualty impact that any attack could achieve.

4. Agreement that photography be restricted to public areas only.

Following on from any contract agreements a site can also consider some of the following advice to enhance its digital look and feel to discourage attack planning:

Stage Management:

1. Consider the placement of your overt security teams at key points. Areas to consider would be at entrances (To enhance the impression of the security regime) and front of house/back of house access areas.

2. Moving your security teams around the site so it appears that there are more staff employed than are actually in place.

3. Placement of positive customer care and security posters and messages.

Engagement:

1. Have security staff and customer service agents being photographed in positive engagement scenes with customers. To a potential attacker this will indicate that approaches and interaction is made with customers and is again discouraging to them.

2. If the site has an onsite Police team, then photographs of joint security/police patrolling should be encouraged.

This advice is not intended to be prescriptive but to guide to reasonable mitigations to reduce any security implications.

Ultimately, the decision to allow the imagery activity to take place is a matter for the site owner

NaCTSO

National Counter Terrorism Security Office, PO Box 849, London, SW1P 1XD
02079317142, www.nactso.gov.uk, nactso@cpni.gsi.gov.uk