

ACPO SECURITY SYSTEMS POLICY 2004

EXPLANATORY NOTES

(Paragraph numbers relates to the policy document)

Introduction

The direction which the policy revision and the work leading to it has taken can be summarised as follows:

To reduce the number of false calls passed to the police.

To relate the policy to police response to electronic security systems to which police response is sought, not just intruder alarms.

To place technical requirements into nominated standards and codes of practice.

To place responsibility for compliance with those standards in the hands of approved Independent Inspectorates. Enforcement of standards should not be a police function.

To place the supervision of those Independent Inspectorates under UKAS standards.

Subject to future introduction of legislation to regulate the private security industry, to have requirements for conviction checks and related matters currently within this policy, incorporated into such legislation.

To avoid the repetitive discussions over technical and administrative matters which do not effect the nature of police response or the level of false calls passed to the police.

The following explains the changes in policy and paragraph references relate to the same paragraph number in the new policy draft. It is not intended that it shall be published with each copy of the policy but available to assist response to enquiries.

- 1.1 The policy is no longer only applicable to intruder alarms and recognises that technology may be blended for specific situations. The policy now extends to CCTV security systems on private premises and stolen vehicle tracking systems.
- 1.2 Technical standards are in preparation for stolen vehicle tracking systems but such systems are already operating and requesting police response. Pending the adoption of agreed standards, it is expected that tracking companies comply where possible with the spirit of this policy and pre-existing ACPO requirements, such as the ACPO Guide to Tracking Companies which has been circulated to tracking companies.

Extending the policy may lead to requests for registration of people tracking systems. Such technology already exists and it is considered better to have an embracing policy which gives the police service a basis upon which to deal with the technology and refuse response to poor systems. The development of standards and operating procedures are essential before this people tracking can be embraced by the service.

- 1.3 Whilst ACPO would seek observer status at board meetings of the inspectorate bodies, it is not appropriate to have full board member status, nor is it possible to participate in every technical forum. The police service should not inspect the Inspectorates and this will be done by UKAS (United Kingdom Accreditation Service) against BS EN45011 and the ACPO Requirements for Security Systems. This document calls up the standards for the relevant sector (CCTV, alarms, vehicle tracking) of the industry. It also establishes the arrangement under which NACOSS will comply with the ACPO / BSEN45011 requirements through their existing BSEN/45012 compliance.

2.1 The purpose of a URN for tracking companies (not each vehicle) is to establish the bona fides, system type and call back numbers of the company, not the vehicle. Standards are under development with police input at a European level. In the meantime such companies have been required to adopt an ACPO Guide on tracking systems. Once details of standards are known, companies in these sectors will be given a time-scale within which to comply. There is limited impact from this technology at present (the current genuine call rate is in excess of 95%). Tracking reports must be confirmed by a stolen vehicle crime reference. The present objective is to set down principles and draw the technology into our policy whilst standards are being written and before the technology becomes commonplace. Whilst some Alarms Administrators are sceptical about this development into other systems, all forces are currently responding to tracking calls and many forces already operate the URN system for this technology. It will be necessary to split the call records for annual statistical purposes to show results for types of security system. Failure to do so will result in intruder alarms appearing to improve through the genuine calls arising from CCTV and tracking.

Where the force system can handle the facility, Urns should be issued per discreet system, not the premises. E.g. single occupancy building with separate intruder alarm for the building and CCTV for the exterior with a secure perimeter should have 2 Urns. If the CCTV is integral to the alarm as the means of confirmation then only 1 URN applies.

2.1 The attachment of confirmation technology to a Type B system does not automatically make it Type A. It must conform to all aspects of the policy.

3.2 Confirmation Technology

(I) There are reservations within the security and insurance industries that a requirement for confirmed alarms will solve the false call problem. The adding of a sequential or audio detector to one circuit of a complex alarm does not qualify the whole system for police response. It is the alarm message to the police, which must be confirmed. It is recognised that Arc's and insurers may have to specifically agree with the customer what the controller is to do with the unconfirmed calls. New installation configurations may need to be developed and codes of practice modified. Hence the lead-in time for adoption. Police force systems will also have to be able to record, which systems are confirmed and have this information available to call handling staff.

(ii) It is noted that some other European countries successfully operate confirmed response. The false call rate for this technology in the UK has improved and to some extent it is not used correctly because unconfirmed calls are still passed to the police and so increased the false call statistics for this type of installation. Some police forces are under such pressure from local communities that giving an alarm system with a 90% false call rate a level 1 response is not acceptable. There is a risk in some forces that all alarms calls could be downgraded to level 2 at best. The objective is to keep calls with a higher probability of being genuine in the level 1 response category.

3.3 This section will apply for systems breaching the withdrawal of response threshold. Existing systems will not be required to invest in additional technology until they breach the withdrawal threshold.

If an alarm has dual signalling and both line contacts are lost, or a line is lost followed by intruder detection on second signal path, then this is treated as a confirmed activation.

3.9 Personal attack alarms

(I) The reference to exact location is to take account of the development of portable p.a. systems. For fixed systems in premises the site of the p.a. device would be pre-determined and the "exact location" would be the address of the building (no change), whilst for vehicles, or other portable devices some form of location device, such as GPS (global positioning system) would be required. The location data would have to be in a format, which was meaningful to the police. This is being addressed under the CEN278 WG14 vehicle-tracking standard.

- (ii) BSIA has produced a 10-point plan to reduce false calls from personal attack alarms. This should be implemented by March 2005. Point 2 of this plan relates to the threshold of false calls being reduced from 5 to 2 in a rolling twelve month period. (There is currently a pilot scheme taking place by a selection of both urban and rural forces, to be reviewed in March 2005).
- (iii) A definition of p.a. call and misuse is now included at 3.9 in the policy and should be included in letters to customers on issue of EARN.

3.11 Under the previous policy an alarm could reach withdrawal of response though misuse of the p.a., which was then, permitted extra calls whilst the intruder element was banned. This new section allows for discretion as to the element, which is withdrawn. It is accepted that some police forces may not be able to accommodate this.

3.12 Type B Security Systems.

Local crime trends and intelligence reports may dictate that on a case by case basis response is desirable. However, country-wide statistics indicate false call rates of 99% and that forces have successfully filtered over 50% of Type B calls for little risk of burglary. As a result of the significant resource commitment generated by Type B systems, which are often not subject to the same standards and policy requirements as Type A, it is suggested that force crime prevention advice encourages the installation of Type A systems rather than Type B.

4.1.b Appendix C - Conviction checks.

This has been modified to cover persons who install and service other security systems to which the policy applies. It is suggested to police forces that replies to requests under this section should state “meets / does not meet the requirements of the ACPO Security Systems Policy” rather than “has/ has no convictions”. This section was introduced to avoid persons of dishonest or violent background from gaining access to premises and security information. Particularly with the adoption of the Human Rights Act it is considered that the convictions should be relevant to protecting the security of the customer. For example, theft, burglary, dishonesty, supplying of drugs, offences of indecency and serious assault would certainly be relevant, but drink/drive convictions would not unless they were crime-related. Juvenile convictions also require consideration as to their relevance to the current application.

Conviction checks should normally be carried out in the force area where the employer is based. There should be no reason to carry out subsequent checks in other force areas.

Checks should be limited to convictions only – enhanced checks are not required. Cautions are an admission of guilt but not a conviction. Where forces are concerned that cautions may be relevant or there is information that would make the applicant unsuitable, forces may deem the applicant unsuitable. However, a member of that force must be prepared to give evidence in court to justify this decision. Non-conviction information may only be disclosed on the authority of an officer of ACPO rank. Alarms administration units must establish their procedures for managing this process and any appeals arising from rejected applications.

Enforced Subject Access: When the Criminal Records Bureau are capable of issuing basic level criminal record disclosure certificates and the Secretary of State makes an order prohibiting an employer requiring an employee to obtain a copy of their own criminal convictions under the Subject Access Provisions of the Data Protection Act, this requirement by the employer will become illegal.

The process under the Security Systems Policy is not the same as an individual being required to exercise their rights by an employer. Therefore conviction checks as per Appendix C can continue.

4.2 Information to customer.

This is primarily for the security industry to address. A sample is attached to the guide note for those forces, which may wish to retain the use of this document, the wording is for local decision and does not form part of the policy.

4.3 Monitoring this is problematic and it is for the company to take responsibility for what it says to its customer.

5. & Appendix F. URN application / variation forms:

- (i) Where a premises have an existing URN, a request to transfer the URN to another alarm company or ARC may be made by the customer or the new alarm company supported by the customers authority. It is not necessary to have correspondence from the original alarm company as they are often obstructive when losing a contract. However, a period of 28 days grace should be allowed before the URN is deleted, to enable the new maintaining company time to submit their Appendix F.
- (ii) 3rd party remote ATM sites (cash machines) could qualify for separate URNs if using a separate signalling path, but not if using an extra zone of the alarm system for the premise. Such 3rd party sites often suffer from inadequate keyholder access and inadequate security of the enclosing premises.
- (iii) Premises which are part of a national company / group should be able to elect to have all alarm correspondence sent to a central point. It is claimed by retailers and financial institutions that local failings may be corrected faster via Group Security who are often unaware of the problem.

Appendix G – Hazard & Site Risk Statement (Health & Safety)

- (i) It is a requirement for site risks to be identified and updated by the occupiers of all premises. This arises from concern for officer protection and should be available on the URN file for officers attending. The form only lists a few examples as an attempt at a definitive list may be taken to suggest that situations not listed are free of risk. It is not intended that there should be any site inspection by the police.
- (ii) Appendix G will be submitted with the original URN application (Appendix F) and must be updated whenever changes in risks occur. There is no requirement to submit this form when occupiers change alarm company.

6.3 Keyholders

It is not the intention of this penalty clause to create a record for every incident. Where officers leave the scene prematurely or are re-deployed to other incidents before the keyholder arrives, no further action is required. It should be enforced only when officers at the scene require keyholders, but they do not attend within the required time-scale.

7.3 Sounder delay.

The request for removal of bell delay should not be unreasonably withheld and local police response times are critical to this decision.

9 and Appendix E Administration Charges:

- (I) It is considered that the policy should state the extent of administration charges and those forces which choose not to apply them would state so at Appendix A.
- (ii) The proposed URN administration fee is assessed at £35.00 inclusive of VAT, reviewed after 2 years. This would apply to all applications for a URN and all applications for a URN to be re-instated following deletion. Forces, which choose to issue a second URN in addition to the alarm to cover the p.a., should treat this as a single application and fee.

Ex-directory alarm lines to police HQ may be operated at premium rates to generate income commensurate with line usage. It would be a matter for forces to choose whether to retain the existing annual line charge to each ARC or to opt for premium rate lines. It is not intended they should opt for both.

With the introduction of vehicle tracking and detector activated CCTV systems into the policy, it is in the interest of the police to receive commentary from the ARC/RVRC operator whilst an offence is in progress. The use of premium rate lines may have a detrimental effect on the length of time that ARC/RVRC operators are prepared to spend giving police control room staff information.

- (iii) Whilst researching the site risks issue (Appendix G) it became apparent that the responsibility to disclose such risks should rest with the occupier and completion of this section will involve work on data input. It is therefore appropriate to apply the administration charges to the customer. No fee should be charged for subsequent updating of risk information.

Miscellaneous:

- (i) Appendix A is intended as the point where police forces could list their operational constraints to the policy, such as response times to calls, command & control features, HQ contact numbers, and administrative notes. It is not an opportunity to change the principles of the policy.