



TB 07

February 2001

New ACPO Security Systems Policy

ACPO POLICY ON POLICE RESPONSE TO SECURITY SYSTEMS

1. INTRODUCTION

1.1 The Association of Chief Police Officers (ACPO) of England, Wales and Northern Ireland recognise the rapid development of technology and its use within security systems. This policy details the police response which can be expected to an electronic security system which is identified in the ACPO “Requirements for Security System Services”.

1.2 To enable a security system to be recognised within the ACPO Requirements for Security Services it must comply with the ACPO Policy on Response to Security Systems and a recognised standard or code of practice controlling manufacture, installation, maintenance and operation. Such standards must be in the public domain and not be product based.

1.3 The installation and services provided by the installing company and an alarm receiving centre / monitoring centre, shall be certified by a UKAS accredited certification body in accordance with the provisions of the ACPO Requirements for Security Services.

1.4 It should be noted that police response is ultimately determined by the nature of demand, priorities and resources which exist at the time a request for police response is received.

2. SCOPE OF POLICY

2.1 Type A Remote Signalling Systems.



Systems terminating at BS 5979 (latest draft) recognised alarm receiving centres and system monitoring centres (ARC's);

Systems operating via police control rooms with the specific approval of the Chief Officer of Police.

Unique reference numbers (URNs) will be issued to these systems. In the case of stolen vehicle tracking systems the URN will be issued to operating company or monitoring centre, not to each vehicle.

2.2 Type B Security Systems.

Systems, for which police attendance may be requested, and which operate outside the procedures identified at Section 1 and Type A requirements.

Unique reference numbers will not be issued to these systems.

3 POLICE ATTENDANCE

3.1 For security systems there are three levels of police intervention.

LEVEL 1 Immediate.

LEVEL 2 Police response is desirable but attendance may be delayed, e.g. due to resource availability.

LEVEL 3 No Police attendance, keyholder response only.

3.2 Type A Systems.

The police service has adopted a policy on the use of confirmed alarm technology as part of the effort to reduce false calls. The key stages and time-scales are as follows.

3.3 On introduction of this policy security systems which are, or become, subject to withdrawal of police response will only qualify for restoration of response if messages passed to the police are confirmed. As from October 2001 all new installations will only qualify for URN and police response if messages to be passed to the police are to be confirmed.

3.4 Security systems issued with a Unique Reference Number (URN), including systems installed prior to adoption of this policy will receive LEVEL 1 response until two false calls have been received in a rolling 12 month period.

3.5 Following two false calls in 12 months the police response will move to LEVEL 2 and the customer will be advised in writing. Following five false calls in 12 months LEVEL 3 will apply and police response will be withdrawn. The occupier will be advised



in writing and the installing company will be required to instruct the ARC not to pass alarm messages to the police. This will remain valid until the system has been free of false calls for 3 months.

3.6 Following withdrawal of response, police response may be restored following 3 months free of false calls. To restore response the occupier or the security company shall apply in writing to the Chief Officer of Police, supported by evidence from the security company that the system has been free of false calls, that the original cause has been rectified and the system has been upgraded so that only calls identified as confirmed may be passed to the police. After police response has been resumed only activation's which have been confirmed will be passed for police attendance. Should the level of false calls result in the restoration of response being delayed for more than 6 months the URN will be deleted and the occupier and the security company advised in writing.

3.7 ACPO will invite representatives of relevant organisations to assist in the monitoring of the effect of confirmed technology and to make recommendations to update the policy and / or relevant codes of practice.

3.8 Personal attack alarms (deliberately operated devices).

A personal attack alarm may be operated to summon urgent police assistance when an assailant enters a previously defined area with the obvious intention of harming or threatening any person within that defined area . If the device is portable it shall contain technology to enable the exact location to be determined. These devices may not be used to summon assistance in circumstances other than this. Misuse to summon police attendance to non-attack incidents may result in Level 3 response.

3.9 In a system with both personal attack (deliberately operated) and security systems, the remote signal shall differentiate between the two types. Unless this distinction is made, any withdrawal of Police response sanction will apply to all p.a. calls from the system.

3.10 Personal attack (p.a.) systems conforming to section 3 will attract LEVEL 1 response. Where the threshold for withdrawal of police response is reached the withdrawal will apply to the facility (intruder or p.a.) which has caused 3 or more of the false calls. That part to which response has not been withdrawn continues to receive response until it reaches the withdrawal threshold in its own right. Police response is then withdrawn, but will count from the original withdrawal date so that application for restoration is contemporaneous for both facilities.

3.11 Type B Security Systems



To obtain police attendance, Type B systems will require some additional indication that an offence is in progress or local circumstances which indicate that police response is required. This will usually require human intervention such as member of public, owner or agent visiting, or viewing the premises and the level of police response will depend on the quality of the information received. The addition of electronic means to provide confirmation will not promote such systems to Type A or automatically achieve police response.

3.12 Automatic dialling equipment must not be programmed to call police telephone numbers. Calls handled by non-compliant central stations will be LEVEL 3 response unless supported by additional evidence of an offence being committed as at 3.11.

4 LIST OF COMPLIANT COMPANIES INSTALLING TYPE A SECURITY SYSTEMS

4.1 To identify companies conforming to this Policy it is necessary for each Police Force to hold a list of policy compliant companies. Inclusion on the list does not amount to confirmation that the company or its work has been inspected by the Police. Only companies so listed may install and maintain Type A systems in the particular Police area. Where a company loses police recognition under the policy, its existing customers will have 12 months in which to make alternative maintenance/monitoring arrangements.

Companies apply for inclusion using Appendix B and shall:

- (a) Be inspected and recognised by an independent inspectorate body as at paragraph 1.
- (b) Not have as a principal or employ in the surveying, sale, installation or maintenance of security systems, persons with criminal convictions (other than spent convictions). Appendix C sets out a procedure for the implementation of this requirement. It is a matter for individual Chief Constables to adopt this procedure and such adoption will be identified at Appendix A.

4.2 Information to Customer

The compliant list is for police administrative purposes. Members of the public seeking advice from the police about companies capable of installing remote signalling alarms will be advised to seek information from inspectorate bodies directly.

4.3 Notice to Customer Type A Systems

Prior to the signing of contract the installing company shall give to the customer a



document outlining the Police Policy.

5. NOTICE TO INSTALL TYPE A SECURITY SYSTEM

5.1 Notice of intention to install a Type A security system requiring a URN, shall be sent to the Chief Officer of Police in the form of Appendix F.

This will result in the issue of a Police Unique Reference Number (URN) which must be quoted in any communication regarding the installation. An activation received from an ARC without a current police URN will be treated as a Type B system and not receive a police response without additional evidence of an offence in progress.

Facilities for inspection of the installation shall be made available if required by the Chief Officer of Police.

5.2 Variations

Any variations to the original URN application details shall be notified within 14 days to the Chief Officer of Police in the form of Appendix G.

6. KEYHOLDERS

All premises with Type A systems shall have at least two keyholders, details of whom will be maintained by the ARC or through arrangements with a central keyholding service. Keyholders shall be trained to operate the alarm, be telephone subscribers, have adequate means of transport to attend the premises at all hours, shall have access to all relevant parts of the premises and shall be able to attend within 20 minutes of being notified. Failure to comply may result in withdrawal of police response.

7. DELAYS OF AUDIBLE SOUNDER AND ALARM ACTIVATED SECURITY DEVICES

7.1 Save for as outlined at 7.2 there is no requirement for security systems to have audible or visual warning devices delayed following activation of the system.

7.2 Intrusion detection systems in commercial premises may be required to have audible and visual alarm warning devices delayed for a maximum of 10 minutes where the chief officer of police determines that the call handling time, location of premises and the Force Service Standard would enable officers to attend the premises within that time. (See Appendix A)



7.3 Occupiers of premises within such a 10 minute delay area may apply to have this requirement waived due to individual circumstances.

8. FALSE ALARM MONITORING

8.1 There is an obligation on the part of the installer, maintenance company, customer and the monitoring centre to employ all possible means to filter out false calls. Companies installing Type A systems will have their performance judged on their false call rate. This may be achieved by use of a formula and referral to the installers inspectorate body as set out at Appendix D. The Force may determine whether the formula will be based on police statistics or on those supplied by the company.

9 ADMINISTRATIVE CHARGES

The current policy on charging is set out at Appendix E.

10 MISCELLANEOUS PROVISIONS

10.1 Data Protection Act 1998

Data supplied to the Chief Officer of Police in relation to intruder alarms may be held on a computer and companies should notify clients that (a) limited data supplied by them may be held on Police computers and (b) where the data is relevant to a complaint, it may be disclosed to the relevant independent Inspectorate body recognised by ACPO.

Information supplied must be accurate and kept up to date. Any alterations to the personal data supplied by Alarm Companies must be notified to the Chief Officer of Police within 14 days.

10.2 Advertising

Companies shall not use terminology which might raise in the mind of the customer a guaranteed or unrealistic expectation of police response to a security system and shall not use an ACPO logo or reference in advertising material without written permission from the ACPO General Secretariat, or a police force logo without the permission of the relevant chief officer of police.

11. FINAL DISCRETION



11.1 The policy does not impose any liability on this Force, its officers or employees or the Police Authority arising out of any acts or omissions connected with the alarm installation, including failure or timeliness in responding to any activation's. The Chief Officer of Police reserves the right to:·?

- (a) refuse to admit a company to the compliant list.
- (b) refuse to issue a Police URN for any installation.
- (c) refuse Police response to any security system installation.
- (d) to alter, amend or add to this policy as necessary through the ACPO Security Systems Group.

11.2 Issues which may require amendment to this policy must be forwarded to the Chairman, ACPO Security Systems Group, the address of whom may be obtained from Police Headquarters. The Chairman meets with representatives of the security industry, independent inspectorate bodies, the Association of British Insurers and the British Retail Consortium and other representative organisations to review such matters.

11.3 The ACPO Security Systems Policy is the copyright of the Association of Chief Police Officers (ACPO). No part of this document or the Appendices may be reproduced or offered for sale without the written authority of the Chairman of the ACPO Security Systems Group.

ACPO SECURITY SYSTEMS POLICY 2000
LAST REVISION 10/2000

APPENDIX A: (Example. Remains as at present with force response policy and will include the adoption of options to check convictions and make administrative charges. It should not be used to introduce changes to the principles of the policy.)

Force crest, Chief Officer's name and Headquarters Address

The ACPO unified intruder alarm policy has been adopted by the
Police/Constabulary. The following variations permitted under the terms of the policy apply in this police area.
(Examples)

The Chartered Institute of Loss Adjusters 36 Monument Street London EC3R 8LJ Whilst great care is taken to provide accurate and helpful information and advice in this technical bulletin, readers are expected to check all essential information and to seek advice from appropriate professionals and experts as required



1. Automatic 999 dialling alarm equipment is not permitted.
2. All central monitoring station alarm messages must be transmitted to our Force Control Room, Police Headquarters on dedicated ex-directory telephone lines. The number of which will be disclosed on receipt of a signed contract ...(details of any annual fee/ premium rate charges).
3. The Police/Constabulary Service Standard is to aim to attend all urgent calls within 10 minutes in the following areas :? and town centres. Commercial premises in these areas must have a 10 minute audible sounder delay on remote signalling systems. In all other areas an instant sounder is permitted. In exceptional circumstances companies may apply in writing for exemption to the delay requirement according to individual risks.
4. Commercial alarm companies must enclose a stamped addressed envelope with all correspondence requiring a reply.

All correspondence should be addressed to the Supervisor, Alarm Administration Department,(address).

The Unique Reference Number (URN) must be quoted in all correspondence. In the interests of maintaining security of records all enquiries concerning individual alarm systems must be made in writing. Telephone enquiries regarding systems or particular alarm activations will not be accepted.

Last Revision 10/2000

POLICY AGREEMENT FORM APPENDIX B

This form must be signed by an authorised person at the company head office.

I have read the (name of force) Police Security Systems Policy and Requirements for Security Services. I agree to comply with every requirement of these documents.

I acknowledge that failure to comply will result in my company no longer being accepted by the (name of force) Police or being included on the (name of force) Police list of compliant companies.

I am authorised to sign this document on behalf of (name of



company).....

My company is inspected by the following
organisation:.....

for the following types of security
system.....

Signature.....

Print Full Name

Date.....

Name of Company.....

Position in Company

Address

.....

.....

Post Code

Telephone Number

Fax Number

email address.....

TO BE RETURNED TO: Alarms Administrator

() Police

Police Headquarters

(Address)

The Chartered Institute of Loss Adjusters 36 Monument Street London EC3R 8LJ *Whilst great care is taken to provide accurate and helpful information and advice in this technical bulletin, readers are expected to check all essential information and to seek advice from appropriate professionals and experts as required*



Data Protection Act 1998

Personal data supplied on this form may be held on, and/or verified by reference to information already held on computer

APPENDIX C

DISCLOSURE OF CONVICTIONS

It is suggested the procedure should only be entered into with companies on the List of Compliant Security System Installers of a Police Force or a company making a bona fide application for admittance to the List.

It is emphasised the Rehabilitation of Offenders Act 1974 applies, and 'spent' convictions are not a consideration in the procedure.

The intention is to curtail those with criminal convictions having access to premises and information relating to the security of premises. The offences should therefore be relevant, such as involving theft, dishonesty, serious assault and drugs.

PROPOSED PROCEDURE

(i) Police checks must not take the place of normal recruitment procedures. References should be required and taken up in the case of all new appointments, with unexplained gaps in employment being satisfactorily accounted for.

(ii) Each applicant seeking employment where their duties will include surveying, sales, installation and maintenance of security systems with a company on a Force's List of Compliant Intruder Alarm Installers, or a prospective company wishing to go on the List, will be required to complete a form. The form will be consistent with the model layout as shown at Form A. This will be done after selection, but before appointment.

(iii) Employers may wish to make a statement available to people who may be subject to a criminal records check under these arrangements, to reassure them that ex-offenders will not automatically be rejected. A model statement is offered at Form B.

(iv) The police should not be asked to confirm criminal records where the person concerned has admitted a conviction which would clearly render him or her unsuitable to install intruder alarm systems.

The Chartered Institute of Loss Adjusters 36 Monument Street London EC3R 8LJ *Whilst great care is taken to provide accurate and helpful information and advice in this technical bulletin, readers are expected to check all essential information and to seek advice from appropriate professionals and experts as required*



- (v) If a police check is then considered necessary, the employer should then pass the request on to the Chief Constable of the Police Force for their area.
- (vi) Employers should make every effort to confirm the identity of the applicant before the police are required to process the check. Verification of identity, date of birth, and any change of name should be obtained.
- (vii) All applicants must give written permission for the police to institute checks and also advise employers where they consider an applicant unsuitable within the terms of the Policy.
- (viii) The police check will be limited to a PNC check against criminal convictions only. The police will reply stating the person is suitable or that these details appear identical with a person who is considered unsuitable. Details of convictions will not be passed on to the employer.
- (ix) Where a person wishes to complain about this decision on the grounds they have been incorrectly identified, they should have an opportunity to make representations to the police. This should be done in the first place through the employer. Where such a complaint is received by the police, the grounds for rejection will be disclosed to the complainant, but not the employer.
- (x) Where appropriate, the company should be informed they cannot be retained on, or admitted to, the List of Policy Compliant Companies as the Company Conditions section of the Policy has applied.
- (xi) This Policy only applies to new employees of existing companies on the Compliant List and to any prospective company wishing to go on the List. Police Forces may, however, utilise this procedure if someone who is working for a company on the Policy Compliant List is subsequently identified as being unsuitable through his/her criminal convictions. The subject of the report should be informed.

APPENDIX C(continued)

FORM A TO BE RETAINED BY THE POLICE

REQUEST FOR A POLICE CHECK IN RESPECT OF AN

The Chartered Institute of Loss Adjusters 36 Monument Street London EC3R 8LJ *Whilst great care is taken to provide accurate and helpful information and advice in this technical bulletin, readers are expected to check all essential information and to seek advice from appropriate professionals and experts as required*



APPLICATION FOR EMPLOYMENT AS A SECURITY SYSTEM INSTALLER

PART A -? To be completed by the applicant in BLOCK CAPITALS

I am aware that this employment is subject to a police record check and I consent to such a check being performed. This has been explained to me and I understand spent convictions are not considered by the police in assessing my suitability. I authorise the police to inform my employer if they consider me to be an unsuitable employee under their Force Policy on Security Systems, because of any criminal convictions.

Signature Date

Surname/Family Names

All First Names

Maiden/Former Names

Date of Birth / / Place of Birth Sex M/F

Present Address

.....

.....

Previous Addresses in last 5 years (give dates):

.....

.....

(continue overleaf if necessary)

Have you ever been convicted at a Court for any offence which is not now spent under the terms of the Rehabilitation of Offenders Act 1974. YES/NO



If YES, provide details overleaf, including approximate date, the offence, and the Court or Police Force which dealt with you.

APPENDIX C (continued)

PART B -? To be completed by the employer

The person identified above satisfied the conditions for requesting a police check set out in the ACPO Policy on Security Systems. The particulars provided have been verified and I am satisfied they are accurate.

SIGNED DATE

PART C For Police use only

PNC/NIB Records only have been checked against the above details:

lqqqqqqqqqk

x x

x x No trace on details supplied.

mqqqqqqqqqj

lqqqqqqqqqk

x x The subject appears identical with the person

x x whose criminal record is attached.

mqqqqqqqqqj



SIGNED DATE

ALL FORMS TO BE RETURNED TO THE NOMINATED OFFICER IN THE FORCE FOR IMPLEMENTATION OF THIS ACPO SECURITY SYSTEMS POLICY.

THIS FORM MUST BE RETAINED BY THE POLICE

.....
.....

APPENDIX C(continued)

FORM B

DISCLOSURE OF CRIMINAL CONVICTIONS

NOTICE TO:

The Police, in applying their policy on intruder alarms, may preclude a company from its List of Compliant Security Systems Installers if a principal or employee has criminal convictions.

In connection with your employment/application for employment, you are required to supply the personal information. Any convictions, including bind-overs, should be shown. You are required to sign the form authorising the Police to inform your employer if you are considered to be unsuitable for employment under the terms of their Security System Policy.

It should be noted that failure to provide relevant information, or to give false information, could lead to prosecution for an offence under Section 16, Theft Act 1968.

The Chartered Institute of Loss Adjusters 36 Monument Street London EC3R 8LJ Whilst great care is taken to provide accurate and helpful information and advice in this technical bulletin, readers are expected to check all essential information and to seek advice from appropriate professionals and experts as required



Following the checks the Police, at their discretion, may advise an employer/ prospective employer that an individual is not acceptable because of their convictions but in so doing they will NOT reveal actual details.

Where you believe you have been wrongly identified, you are entitled to make representation to the Police. This should be done through the employer in the first instance.

If there is insufficient space on the form overleaf to fully answer any question, please continue on a separate sheet of paper.

NB THE REHABILITATION OF OFFENDERS ACT 1974 APPLIES TO THIS REQUEST FOR INFORMATION. YOU ARE NOT REQUIRED TO DISCLOSE A CONVICTION WHICH HAS BECOME SPENT UNDER THE ACT.

Last revision 10/2000

FALSE ALARM MONITORING FORMULA APPENDIX D

The following formula may be used to monitor the performance of companies installing remote signalling alarms
upper action level =

a = the force false alarm rate for a particular reference period (e.g. 28 days, month or year)

N = the number of installations for a particular company

Z = the value taken from tables based on normal distribution. The figure of 1.64 has been chosen to give the following producers risk and consumers risk.

Producers risk - the probability of wrongly identifying as inefficient a company whose false alarm rate is the same as the force rate is 1 in 8000.



Consumers risk - the probability of wrongly identifying as efficient a company whose false alarm rate is the same as the upper action level is 7 in 8. This would be less for companies operating above the upper action level.

NB. Each installing company will have a different upper action level dependent upon their total number of installations.

Mode of application

The application of the formula is only a guide which will intimate to those monitoring performance that a problem may need to be addressed.

Where a company has a false alarm rate which exceeds the upper action level for that particular company for 3 consecutive months or for any 6 months in a rolling 12 month period the following procedure will apply.

The alarm installation / maintenance company will be notified in writing that their false alarm rate exceeds their upper action level. They will be requested to reduce their false alarm rate to inside of their upper action level within 3 months. The companies inspectorate body will also be informed.

(i) Where a claim is made that the upper action level has been exceeded on the grounds of unique types of alarm installations a revised rate may be introduced at the discretion of the Chief Officer of Police. Where the Chief Officer considers a claim for a revised upper action level is unacceptable he may refer the matter to the appropriate independent inspectorate for arbitration.

(ii) Where a reduction to the false alarm rate is not achieved within a three month period the Chief Officer will consider the following options-

(a) if the company appears to have made little or no effort to resolve the problem an immediate withdrawal of facilities to acquire new unique reference numbers (URNs) will take place until the company has reduced their false alarm rate to within their upper action level. The circumstances will be reported to the appropriate inspectorate body as a serious non-compliance with the ACPO Requirements for Security Systems Services document..

or

(b) if the company demonstrates it has tried but been unsuccessful in reducing their false alarm rate to within their upper action level the circumstances will be reported to the



appropriate inspectorate body as a non-compliance. The Chief Officer may agree objectives with the company to resolve the matter, in such cases the URN facility will not be withdrawn.

Last revision 10/2000

ADMINISTRATION CHARGES APPENDIX E

The following charging structure is adopted by all police forces seeking to recover administration costs in respect of security systems. Payment shall be made to the individual police force in accordance with arrangements set out at Appendix A.

1. Each application for a Unique Reference Number is subject to an administration fee payable by the system user. Forces may determine the charge up to a ceiling of £30.00, inclusive of VAT. The fee is identified at Appendix A and the ceiling will be reviewed every two years by ACPO.
2. The URN will not be given to the alarm company until the customer's cheque in respect of the URN administration fee has cleared and the completed application form accepted. Incomplete URN applications will be returned un-processed.
3. The administration fee is payable for new URN applications, new occupiers of premises taking over existing security systems and applications for re-issue of a deleted URN.
4. In the event the installation does not proceed after the URN has been allocated, the fee is non-returnable.
5. All security system monitoring centres operating under this policy must utilise the dedicated ex-directory lines nominated by each police force. An access fee may be chargeable and will be recovered by either a) the use of premium rate telephone call charges (0897) or b) an annual fee. The method chosen by the force is detailed at Appendix A.
6. Caller line identification is operated and central stations must not bar this facility on police calls.
7. If a stamped, addressed envelope (SAE) is required with the URN application this will be listed at Appendix A.



These administration charges do not represent a charge for our attendance at alarm calls, nor do they form a contract with the occupier of the premises for response to calls.

Date of last revision (10/2000)

APPENDIX F

NOTICE OF INTENTION TO INSTALL / RE-INSTA TE A SECURITY SYSTEM. STRICTLY CONFIDENTIAL

DETAILS OF INSTALLING COMPANY.....

address..... Tel No

PROTECTED PREMISES:

Name of Householder or Trading Name.....

Type of Business (e.g. Retail, Factory, Office etc.).....

Address (including street number)

.....

County Postal Code

Telephone Number(inc. STD) (i) Premises (ii) Alarm Line (if known)

O/S Grid Map Reference

Directions from Main Road

.....

.....

The Chartered Institute of Loss Adjusters 36 Monument Street London EC3R 8LJ *Whilst great care is taken to provide accurate and helpful information and advice in this technical bulletin, readers are expected to check all essential information and to seek advice from appropriate professionals and experts as required*



TYPE OF SYSTEM i.e. Intruder/ Personal Attack/ Combination / CCTV
State.....

.....

Confirmation Audio Visual Sequential.....CCTV..... Other
(State)

Additional Features linked to Alarm e.g.. Smoke/CCTV/Chemical Trace/Other (State)

.....