



ACPO POLICY ON POLICE RESPONSE TO SECURITY SYSTEMS (APRIL 2006)

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 Systems it must comply with the ACPO Policy on Police 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 (ARC) / monitoring centre, shall be certified by a United Kingdom Accreditation Service (UKAS) accredited certification body in accordance with the provisions of the ACPO Requirements for Security Systems.
- 1.4 Additional operational restrictions by individual forces are outlined within **Appendix A** of this policy.

2. SCOPE OF POLICY

2.1 Type A - Remote Signalling Systems.

- 2.1.1 Systems terminating at a recognised (ARC), Remote Video Response Centre (RVRC) for CCTV and System Operating Centre (SOC) for vehicle tracking. All centres must conform to BS 5979 (Cat II).
- 2.1.2 Unique reference numbers (URNs) will be issued to systems at these recognised centres. In the case of stolen vehicle tracking systems the URN will be issued by ACPO to the operating company or monitoring centre, not to each vehicle.
- 2.1.3 ARCs dealing solely with alarm systems within their own company premises (in-house monitoring), are exempt from the BS5979 Cat II certification provided:
 - a) the facility was operational with police consent prior to 31st October, 1995, and there has been no change of premises; and
 - b) there is no monitoring of any alarm or security device in premises other than those owned by that company, i.e. no 3rd party commercial risk is undertaken; and
 - c) the intruder alarm systems are operated in accordance with all other aspects of this policy.

2.2 Type B - Security Systems.

- 2.2.1 URNs will not be issued to security systems which operate outside procedures identified at Section 1 and Type A requirements.

3. POLICE ATTENDANCE

3.1 Type A Systems

3.1.1 For Type A security systems there are two levels of police intervention.

LEVEL 1 – Immediate/Urgent

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.

LEVEL 3 – Withdrawn

No Police attendance, keyholder response only.

3.1.2 The police service has adopted a policy on the use of confirmed alarm technology as part of the effort to reduce false calls.

3.1.3 All new applications will only qualify for a URN and police response if installed to the current required standard (PD6662).

3.1.4 Security systems issued with a URN will receive LEVEL 1 response until three false calls have been received in a rolling 12 month period.

3.1.5 Following two false calls in 12 months the customer will be advised in writing, with a copy being forwarded to the maintaining alarm company, informing them of the situation and recommending urgent remedial action.

3.1.6 Following three false calls in 12 months LEVEL 3 will apply and police response will be withdrawn. The customer will be advised in writing with a copy to the maintaining company, who will be required to instruct the ARC/RVRC not to pass alarm messages to the police.

3.1.7 Following withdrawal of response, the following conditions will apply in order to reinstate police response:

- (i) Unconfirmed systems will need to be a confirmed DD243 (2004) system (all systems installed prior to DD243 2002 are designated unconfirmed).
- (ii) Confirmed DD243 (2002 / 2004) systems will require the cause of the false alarms identified and remedial action taken.

Reinstatement of police response can be achieved immediately following compliance with the above. Where a system has been upgraded, a copy of the NSI Compliance/ SSAIB Conformity certificate will be required by the police.

- (iii) Systems will have to wait three months free of false calls (supported by evidence from the security company).

The Security Company should apply for reinstatement of response using **Appendix F – Annexe A**.

3.1.8 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.

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

3.2 CCTV Systems

3.2.1 To enable remote detector activated CCTV systems to gain a URN for police response, systems are to be installed to the standards and requirements specified in **Appendix R**.

- 3.3 **Personal attack alarms (PA).**
- 3.3.1 A deliberately operated device, known as a PA, 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 will not require any additional information concerning its location, other than the address of the premises. These devices must 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.
- 3.3.2 Installation of PA's must comply with the BSIA / ACPO Ten Point Plan as specified in **Appendix T**.
- 3.3.3 In a system with both PA and security system, the remote signal shall differentiate between the two types.
- 3.3.4 PA systems conforming to section 3.3 will attract LEVEL 1 response. Where the threshold for withdrawal of police response is reached the withdrawal will apply to the facility (intruder or PA) which has reached the threshold. 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 applies to both parts of the system at the same time.
- 3.3.5 Following withdrawal of response to the PA, the security company should apply for reinstatement using **Appendix F – Annexe B**.

3.4 **Type B Security Systems**

- 3.4.1 The electronic security industry has seen an increase in the availability of Type B alarms (portable personal attack and CCTV systems). These are being sold and bought with the expectation of prompt police attendance. ACPO, whilst not wishing to preclude the ability to provide a prompt response to crimes in action, observe that the development of this technology might if unchecked lead to significant additional demands and higher expectations of police attendance than would be appropriate.
- 3.4.2 To obtain police attendance, Type B systems will require some additional indication from a person at the scene that a criminal offence is in progress which indicates that police response is required. This will require human intervention such as member of public, owner or agent visiting, or viewing the premises. The addition of electronic means to provide confirmation will not promote such systems to Type A or achieve police response.
- 3.4.3 There is no guarantee of police response to Type B systems. Type B calls should be passed to the police by public telephone lines or 999 as appropriate. The level of police response will depend on the quality of the information received.
- 3.4.4 Automatic dialling equipment **must not** be programmed to call police telephone numbers.
- 3.4.5 Calls received from non-compliant ARCs/RVRCs and calls from compliant ARCs/RVRCs without a valid URN **will not** receive a police response unless circumstances outlined in 3.4.2 above apply.

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, maintain and/or monitor Type A systems in the particular Police area. Where a

company loses police recognition under this policy, its existing customers will have 3 months in which to make alternative maintenance/monitoring arrangements.

4.1.2 Companies applying for inclusion on the above list must do so using **Appendix B** and shall:

- (a) Be inspected and recognised by an independent inspectorate body as at paragraph 1.3.
- (b) Not have as a principal or employ in the surveying, sale, installation, maintenance or administration 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 in **Appendix A**.
- (c) Once accepted will take responsibility for ensuring the company updates itself with amendments to the Policy, which are updated in April and October each year.

4.2 **Information to Customer**

4.2.1 The compliant list is for police administrative purposes. Members of the public seeking advice from the police about companies capable of installing remote signalling systems will be advised to seek information from UKAS accredited inspectorate bodies directly as identified in **Appendix H**.

4.3 **Notice to Customer Type A Systems**

4.3.1 Prior to the signing of contract the installing company shall give to the customer a document outlining the Police Policy. (**Appendix I**)

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**.

5.1.2 This will result in the issue of a URN which must be quoted in any communication regarding the installation. An activation received from an ARC/RVRC 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.

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

5.2 **Variations**

5.2.1 The Chief Officer of Police shall be notified within 28 days of any variation to the original URN application details, in the form of **Appendix F**.

6. **KEYHOLDERS**

6.1 All premises with Type A systems shall have at least two keyholders, details of whom will be maintained by the ARC/RVRC 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. The maintenance of keyholders records is the responsibility of the ARC/RVRC, not the police.

6.2 Customers who employ a commercial keyholding company must be aware of the Security Industry Authority Licensing Regulations in relation to keyholding and response.

- 6.3 Failure of keyholders to attend when requested on three occasions in a rolling twelve month period, will result in the withdrawal of police response for a three month period. The procedure for reinstatement will be as 3.1.7.

7. DELAYS OF AUDIBLE SOUNDER AND ALARM ACTIVATED SECURITY DEVICES

- 7.1 There is no requirement for security systems to have audible or visual warning devices delayed following activation of the system. However, commercial premises may be required to have their 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**)
- 7.2 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.
- 8.2 Definition – For the purpose of this policy, a false alarm is an alarm call which would normally be passed to the police and has not resulted from:
- a) a criminal attack, or attempts at such, on the protected premises, the alarm equipment or the line carrying the alarm signal.
 - b) actions by the emergency services in the execution of their duty.
 - c) a call emanating from a personal attack system made with good intent.
- Activation of detectors without apparent damage or entry to the premises and line faults, will be considered as a false alarm unless proved otherwise.

9. ADMINISTRATIVE CHARGES

- 9.1 Each application for a URN is subject to an administration fee payable by the system user. Forces may determine the charge up to a ceiling of £35.00, inclusive of VAT. The fee is identified within **Appendix A** and the ceiling will be reviewed by ACPO every two years. The current policy on charging is set out in **Appendix E**.

10. MEMORANDUM OF UNDERSTANDING

- 10.1 For non-compliance or poor performance by a compliant company or ARC/RVRC, the procedure set out in the Memorandum of Understanding should be implemented before suspension of URNs. (**Appendix J**).

11. MISCELLANEOUS PROVISIONS

11.1 Data Protection Act 1998

- 11.1.1 Data supplied to the Chief Officer of Police in relation to security systems 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 UKAS accredited Inspectorate body recognised by ACPO.

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

11.2 **European Court of Human Rights Considerations**

11.2.1 The policy has been drafted taking into account the appropriate principles of the Human Rights Act 1998. It has also been subject to suitable legal vetting.

11.3 **Freedom of Information Act 2000**

11.3.1 This document is publicly available and published on the ACPO website (www.acpo.police.uk).

11.3.2 Should any requests be received seeking further information about either the policy, its implementation, procedures used by Police Forces or companies, or any other aspect, the request is to be dealt with by the Force Freedom of Information Officer.

11.4 **Racial Equality**

11.4.1 The policy has been drafted taking into account the appropriate principles of Sections 2 (2) and (3) of the Race Relations Act (Statutory Duties) Order 2001. A Race and Equality Impact Assessment is attached at **Appendix U**.

11.5 **Advertising**

11.5.1 Installation Companies, ARC's and Inspectorate Bodies 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.

11.5.2 The use of wording such as 'Police Approved', 'Police Preferred', 'Police Compliant' and 'Meets Police Requirements' must not be used.

12. **FINAL DISCRETION**

12.1 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 security system 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.

12.2 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 British Security Industry Association (BSIA), UKAS accredited inspectorate bodies, the Insurance Property Crime Research Committee (IPCRes) and other representative organisations to review such matters.

- 12.3 The ACPO Police Response to Security Systems Policy is the copyright of the Association of Chief Police Officers. This Policy and Guidance Notes are available on the ACPO website at www.acpo.police.uk and www.securedbydesign.com and may be downloaded for individual use.

INDEX TO APPENDICES

APPENDIX A	POLICY VARIATIONS AND FORCE SERVICE STANDARD
APPENDIX B	POLICY AGREEMENT FORM
APPENDIX C	DISCLOSURE OF CONVICTIONS
APPENDIX D	FALSE ALARM MONITORING FORMULA
APPENDIX E	ADMINISTRATION CHARGES
APPENDIX F	COMBINED NOTICE OF INTENTION TO INSTALL AND VARIATION FORM KEY TO COMPLETION OF APPENDIX F
ANNEXE A	RESTORATION OF RESPONSE TO INTRUDER ALARM
ANNEXE B	RESTORATION OF RESPONSE TO PA ALARM
APPENDIX G	HAZARDS AND SITE RISK STATEMENT (HEALTH & SAFETY)
APPENDIX H	POLICY COMPLIANT COMPANIES – POLICE ADVICE TO PUBLIC
APPENDIX I	LETTER TO POTENTIAL CUSTOMER
APPENDIX J	MEMORANDUM OF UNDERSTANDING
APPENDIX S	REQUIREMENTS FOR SECURITY SYSTEMS SERVICES
APPENDIX T	BSIA/ACPO TEN POINT PLAN FOR PERSONAL ATTACK DEVICES
APPENDIX U	RACE AND EQUALITY IMPACT ASSESSMENT



APPENDIX A

The ACPO unified security systems policy has been adopted by Cambridgeshire Constabulary. The following variations permitted under the terms of the policy apply in this police area.

1. Response Policy 4.1. Companies on either list of policy compliant companies (Maintaining/Monitoring) who are not issued with a URN within 12 months of inclusion on that list, or who have had no live URN's for a period of 12 months will be removed from that list.
2. Alarm companies installing detector activated CCTV systems and Remote Video Response Centres monitoring them must be on the Cambridgeshire Constabulary list of compliant companies for CCTV prior to URN applications being approved.
3. URN's for security systems are issued for a particular subscriber, at a particular premises and for a particular policy compliant company. They are not transferable.
4. Type A Remote Signalling Systems. All Appendix F applications for new URN's must be accompanied by a signed and completed current Appendix G.
5. The 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.
6. Details of all Type A security system activations must be transmitted to the Cambridgeshire force control centre at Police Headquarters on the dedicated ex-directory telephone line. The number of which will be disclosed to Alarm Maintenance Companies on URN Approval. Calls on the premium rate line will be charged at 75 pence per minute.
7. Alarm-receiving Centres must not pass Type B calls by dedicated line. Breach of this condition may result in action being taken against that ARC.
8. Alarm-receiving Centres and Remote Video Response Centres, if requested, will be required to provide information on the total number of URN's being monitored in the Cambridgeshire area.
9. Cambridgeshire Police service standard is to aim to attend all urgent calls within 10 minutes in all urban areas and 20 minutes in all rural areas. All commercial and domestic properties are allowed instant bells. There is no requirement for a delay on any audible or visual warning device at any time.
10. Response Policy Appendix C. Disclosure of convictions applies to all policy compliant companies with an installing branch within the Cambridgeshire Force area. All requests for checks are to be forwarded to the Security Systems Officer at Force Headquarters and include a SAE for the Alarm Company concerned.
11. Response Policy Appendix E. All £35.00 cheques for new URN applications must be made payable to Cambridgeshire Police Authority. Rejected URN applications and associated cheques will be returned to the Alarm Company

POLICY AGREEMENT FORM

APPENDIX B

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

I have read the Cambridgeshire Constabulary 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 Cambridgeshire Police or being included on the Cambridgeshire Police list of compliant companies.

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

..... Position in Company

My company is inspected by for the following types of security system.....(Copy of certificate to be enclosed.)

This policy is a living document, which may be subject to amendment in April and October each year. It is your responsibility to ensure that your company is aware of these amendments. The policy is available on the ACPO website (www.acpo.police.uk).

Signature..... Print Full Name

Date.....

Address

.....
.....
.....

Post Code Telephone Number

Fax Number Email

Our Alarm Receiving Centre(s)

(i) Name

Telephone Number
(for police operational use)

(ii) Name

Telephone Number
(for police operational use)

Please Return to:-

Alarms Administrator, (name of Force) Police Headquarters, Address
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 that 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 that the Rehabilitation of Offenders Act 1974 applies, and 'spent' convictions cannot be considered.

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, drugs and offences of indecency.

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, maintenance and administration of security systems (in accordance with BS7858) with a company on a Force's List of Compliant Security System 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 for employment in the surveying, sales, installation, maintenance and administration of security systems.
- (v) When a police check is required, the employer should then pass the request on to the Chief Constable of the Police Force for their area.
- (vi) Employers must make every effort to confirm the identity of the applicant before the police are required to process the check. They must also confirm the correct spelling of the full name, the date and place of birth and current address.
- (vii) All applicants must give written permission for the police to instigate 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.

APPENDIX C (continued)

- (x) 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. If someone who is working for a company on the Policy Compliant List is subsequently identified as being unsuitable through his/her criminal convictions, police forces may notify the relevant employer. The subject of the report will be informed.

APPENDIX C (continued)

FORM A TO BE RETAINED BY THE POLICE

REQUEST FOR A POLICE CHECK IN RESPECT OF AN APPLICATION FOR EMPLOYMENT WITHIN A SECURITY SYSTEM COMPANY

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.

FORM B

DISCLOSURE OF CRIMINAL CONVICTIONS

EMPLOYER TO HAND THIS FORM TO APPLICANT

NOTICE TO THE APPLICANT

The Police, in applying their policy on security systems, 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.

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.

FALSE ALARM MONITORING FORMULA

APPENDIX D

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

$$\text{upper action level} = \left(a + \frac{1}{N} \right) \left\langle 1 - \frac{1}{9(Na + 1)} + Z \sqrt{\frac{1}{9(Na + 1)}} \right\rangle^3$$

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 company's 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.

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 URN is subject to an administration fee payable by the system user. Forces may determine the charge up to a ceiling of £35.00, inclusive of VAT. The fee is identified at **Appendix A** and the ceiling will be reviewed every two years by ACPO.
2. Upon receipt of the administration fee, a URN will be allocated to the system and issued to the maintaining company. If the applicant's cheque fails to clear, the URN will be cancelled and the security system company informed.
3. The administration fee is payable for:
 - a) New URN applications
 - b) New occupiers/owners of premises taking over existing security systems (false alarm history deleted)
 - c) Applications for re-issue of deleted URNs
 - d) Existing user changing alarm company (system retains false alarm history unless upgraded to DD243 2004
 - (i) Where a security company cancels a URN, a period of 28 days grace should be given to allow another security company to takeover the URN.
 - (ii) Where a security company applies to takeover a URN from an existing company, they may do so supported by the customer's authority.

Where a security company takes over another security company, or a premises changes name only, no charge is made and the systems retain their false alarm history.

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 or b) an annual fee. The method chosen by the force is detailed at **Appendix A**.
6. If caller line identification is operated, 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.

ACPO Policy on Police Response to Security Systems (April 2006)
ACPO POLICY ON POLICE RESPONSE TO SECURITY SYSTEMS

APPENDIX F

NOTICE OF:
 VARIATION REASON(S):

	Installation Date:
	Variation Date:

INT URN	1	
P/A URN	2	
URN	3	

NAME OF ALARM RECEIVING CENTRE	
Police Ref:	
Address	
Tel:	

NAME OF INSTALLER	
Police Ref:	
Address	
Tel:	

NAME OF MAINTAINER	
Police Ref:	
Address	
Tel:	

TYPE OF SYSTEM	

TYPE OF CONFIRMATION	

ADDITIONAL FEATURES	
	TMD

TYPE OF SIGNALLING	
Primary	
Secondary	

STANDARD TO WHICH INSTALLED	

EXISTING URN NO.			
Int		CCTV	
PA		Veh tracking	

PREVIOUS USER (Company name when applicable)	

ADMIN FEE	SOUNDER DELAY

CERTIFICATE NO:	
-----------------	--

Signed: _____
 Print Name: _____
 Position in company: _____
 Date: _____

DETAILS OF PROTECTED PREMISES

HOUSEHOLDER	Title:	Initial(s):	
	Surname:		
	Business Name:		
Trading Name (if different):			
Address:			
Address:			
Town:			
County:			
Postcode:	Tel:	(incl STD code)	
	E-mail address		
Type of Premises:			
If other, state:	O/S Grid Map Ref FIG		
Directions from main road: <i>(Rural / new sites)</i>			

If this form is not completed as appropriate or the Hazard and Site Risk statement or the fee is not enclosed it will be returned unprocessed

POLICE USE ONLY

ACPO POLICY ON POLICE RESPONSE TO SECURITY SYSTEMS

KEY TO COMPLETION OF APPENDIX F DOCUMENT

Select the type of notice, from 1 to 3.

Then select the appropriate data, i.e. if number 1 is selected, you will need to choose data from the headings marked with a 1.

Note: If number 3 is selected choose data relevant to the variation.

- NOTICE OF:**
1. Application for a Unique Reference Number (URN).
 2. Application to reinstate a Unique Reference Number (URN).
 3. Variation to an existing security system.

TYPE OF SYSTEM (1)	TYPE OF CONFIRMATION (1 2 3)	ADDITIONAL FEATURES (1 2 3)	TYPE OF SIGNALLING (1 2 3)
Intruder Alarm	Audio	None	Digital Communicator
Personal Attack	Visual	Smoke Generator	Monitored Line
Combined IA/PA	Sequential	CCTV	Direct Line
CCTV	Audio and Sequential	Lighting	Radio
Vehicle tracking	Visual and Sequential	Chemical trace	Dual Signalling
	Visual and Audio	Access control	
	Visual, Audio & Sequential		
ADMIN FEE (1 2 3)	STANDARD TO WHICH INSTALLED (1)	TYPE OF PREMISES (1)	VARIATION REASON(s) (1 2 3)
Applicable	PD 6662	Retail	Upgrade to confirmation
Not Applicable	BS 4737	Commercial	Signalling amendment
	BS 4737 + DD: 243:2002	Public Sector	New user
	BS 4737 + DD: 243:2004	Licensed	Change of user name
	BS 7042	Domestic	Address amendment
	BS 6799 Class VI	Industrial	Additional features
	BS EN 50131	Bank or Financial	Takeover from another maintainer
	BS EN 50132	Institutional	Change of Alarm Receiving Centre
	BS 8418	Other	Maintenance contract cancelled
			System removed
			Change of sounder delay
SOUNDER DELAY (1)			
0 Minutes			
5 Minutes			
10 Minutes			
15 Minutes			

**APPLICATION FOR RESTORATION OF POLICE RESPONSE
TO AN INTRUDER ALARM**

On receipt of the withdrawal of response letter the alarm company will be required to carry out remedial work in accordance with the Security Systems Policy, and apply for reinstatement using this form.

Although withdrawal of response will not in the short term affect the status of the personal attack alarm, please note that if this situation has not been satisfactorily resolved within 6 months, the unique reference number allocated to your Intruder / PA will be deleted. It is therefore essential that you give this matter your urgent attention.

URN	INSTALLER / MAINTAINER	SIGNATURE	NAME	DATE

The remedial work required will be dependant on the existing status of the system, as follows:

STATUS	REQUIREMENT	COMPLETED
1) Pre DD243 system	Upgrade to DD243:2004	<input type="checkbox"/>
2) DD243 system pre 2002	Upgrade to DD243:2004	<input type="checkbox"/>
3) DD243:2002 system	Find cause, remedy and detail remedial action below	<input type="checkbox"/>
4) DD243:2004 system	Find cause, remedy and detail remedial action below	<input type="checkbox"/>
5) System has been free of false call for a period of 3 months (supported by evidence)		<input type="checkbox"/>

Please note that remedial action as in points 1-4 above is likely to lead to the immediate reinstatement of response, without the 3 month delay.

Cause & details of remedial work carried out:

**APPLICATION FOR RESTORATION OF POLICE RESPONSE
TO A PERSONAL ATTACK/HOLD-UP ALARM**

Although withdrawal of response will not in the short term affect the status of the intruder alarm, please note that if this situation has not been satisfactorily resolved within 6 months, the unique reference number allocated to your Intruder / PA will be deleted. It is therefore essential that you give this matter your urgent attention.

URN	INSTALLER / MAINTAINER	SIGNATURE	NAME	DATE

- 1) Is the PA / Hold-up facility required? **YES / NO**
- (a) If not, and you may need to consult your insurance company, has the device been removed? **YES / NO**
- (b) The facility to signal a PA should also be removed (i.e. disable pin 2) **YES / NO**
- 2) Is intervention in place? **YES / NO**

Please note that the use of intervention is likely to lead to a reinstatement of response without a three month clear period.

Please explain the method of intervention used:

If the PA / Hold-up facility is still required and intervention is not appropriate, an application for restoration of response must be made (using this form) to the Security Systems Administrator, once the following points have been addressed:

- 1) Has the system been clear of false calls for three months? **YES / NO**
- 2) Are all of the PA / Hold-up devices dual action and labelled? **YES / NO**
- 3) Has any duress facility been removed? **YES / NO**
- 4) Has user training been given? **YES / NO**
- 5) Does the PA/Hold-up alarm comply with the BSIA 10-point plan? **YES / NO**
- 6) Details of cause and any other work undertaken to rectify false PA alarms:

HAZARDS AND SITE RISK STATEMENT (HEALTH & SAFETY)

THIS FORM IS CONFIDENTIAL AND MUST BE COMPLETED AND SIGNED BY THE OCCUPIER

Police Officers will not normally enter the premises without the keyholder. However, this may on occasions be necessary due to suspicious circumstances. In order that attending Police Officers may be pre-warned, you are required to state any site hazards or risks.

The following list is not definitive but intended as a guide to some of the most common types of hazards. You should carefully consider your premises and grounds to identify any other risks or hazards and record them under "OTHERS".

MY SECURITY SYSTEMS COMPANY NAME IS:

The following applies to the building(s) and grounds of these premises:

POND	✓		DOGS	✓	
SWIMMING POOL			DANGEROUS ANIMALS		
RIVER FRONTAGE			FIREARMS		
GLASS COPING WALLS			AMMUNITIONS		
RAZOR WIRE			EXPLOSIVES		
INSPECTION PITS			DANGEROUS MACHINERY		
SETTLEMENT TANKS			GAS CYLINDERS		
VATS			TOXIC MATERIALS		
BASEMENT			CONTAGIOUS SAMPLES		
FRAGILE ROOF			FLAMMABLE SUBSTANCES		
DANGEROUS STRUCTURE			FUEL STORAGE		
LOW CEILING BEAMS			CHEMICALS		
SLIPPERY FLOORS			RADIO ACTIVE MATERIALS		
FURNACE			ASBESTOS		
ELECTRICITY SUB-STATION			SPRINKLER SYSTEM		

OTHERS:

IF NO SITE HAZARDS OR RISKS, STATE NONE:

Name of Occupier / Premises	<input style="width: 100%; height: 20px;" type="text"/>		
Address	<input style="width: 100%; height: 20px;" type="text"/>		
County	<input style="width: 90%; height: 20px;" type="text"/>	Postcode	<input style="width: 80%; height: 20px;" type="text"/>
Telephone Number	<input style="width: 100%; height: 20px;" type="text"/>		

I confirm that the Alarm Receiving Centre has been given details of two keyholders capable of attending within 20 minutes of notification. I am aware that persistent failure unjustifiably of keyholders to attend within that time may result in the withdrawal of police response and/or approval for the system.

Signed:	<input style="width: 95%; height: 20px;" type="text"/>	Print Name:	<input style="width: 95%; height: 20px;" type="text"/>
----------------	--	--------------------	--

If commercial business;

State position in Company:	<input style="width: 95%; height: 20px;" type="text"/>	Date:	<input style="width: 95%; height: 20px;" type="text"/>
-----------------------------------	--	--------------	--

POLICE ADMINISTRATION FEE (if applicable) MUST BE ENCLOSED WITH THIS FORM AND RETURNED TO YOUR SECURITY SYSTEMS COMPANY- CHEQUES/POSTAL ORDERS SHOULD BE MADE PAYABLE TO YOUR LOCAL FORCE POLICE AUTHORITY. **PLEASE DO NOT SEND CASH**

The administration charge does not represent a charge for our attendance to activations from your security system nor does it form a contract with the occupier of the premises for response to activations
Should site hazards and risk circumstances change you must update our records (free of charge).

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 H

**POLICE ADVICE TO MEMBERS OF THE PUBLIC
SEEKING INFORMATION ON SECURITY COMPANIES**

To obtain information on companies who supply and install security systems such as Intruder Alarms / Personal Attack Alarms / CCTV systems etc., within your locality, we advise you contact the following Independent Inspectorate Bodies who will furnish you with the relevant details (the Police are not able to provide this information): -

NSI (National Security Inspectorate)

Sentinel House, 5 Reform Road, Maidenhead, Berkshire SL6 8BY

Tel: 0870 205 0000

Fax: 01628 773367

E-mail: nsi@nsi.org.uk

Website: www.nsi.org.uk

SSAIB (Security Systems & Alarm Inspection Board)

Suite 3, 131 Bedford Street, North Shields, Tyne & Wear NE29 6LA.

Tel: 0191 296 3242

Fax: 0191 296 2667

E-mail: ssaib@ssaib.co.uk

Website: www.ssaib.org

Independent Inspectorates are not-for-profit approval bodies who carry out inspection services for the security industry and protect customer interests. They themselves are governed by UKAS (United Kingdom Accreditation Service), the sole accreditation service recognised by the Government.

Please note - if you are also planning to invest in the type of security system that would receive *automatic police response* to its alarm activations, then *only* security companies 'Approved' by an Independent Inspectorate Body *and* who are registered with the Police Force in your locality are permitted to offer this service.

Once you have obtained details from an Independent Inspectorate Body of 'Approved' security companies, who install security systems in your locality to the required European/British Standards, compliant with the ACPO (Association of Chief Police Officers) Police Response to Security Systems Policy, we advise: -

- (a) Before disclosing personal security details, check the address and credentials of the company and proof of identify from their representative.
- (b) You obtain written quotations from at least two security companies.
- (c) Ask if the security company representative can provide you with a list of police rules for occupiers of 'monitored' alarmed premises and also written confirmation that they are currently registered with the Police Force in your area, for the transmission of alarm activations from new installations?
- (d) You ensure that the quotation specifies that the installation will be to European/British Standards for that relevant security system. Also, does it include the terms of maintenance and monitoring contracts?
- (e) Does the company operate a 24-hour call-out service and emergency attendance within four hours?
- (f) Is the installation of a security system a requirement of my insurance company and if so, is the security company acceptable to my insurer?

PLEASE NOTE - When investing in Security Systems for your home or business – it's not advisable to deal with Cold Callers or telesales enquiries – you should avoid doing doorstep or telephone business. If members of the public have serious doubts about the legality or sales techniques being employed by this type of security company, they should contact the Police or Trading Standards for advice.

APPENDIX I

Letter to be handed to potential customers by all companies installing security systems.

Dear Sir/Madam

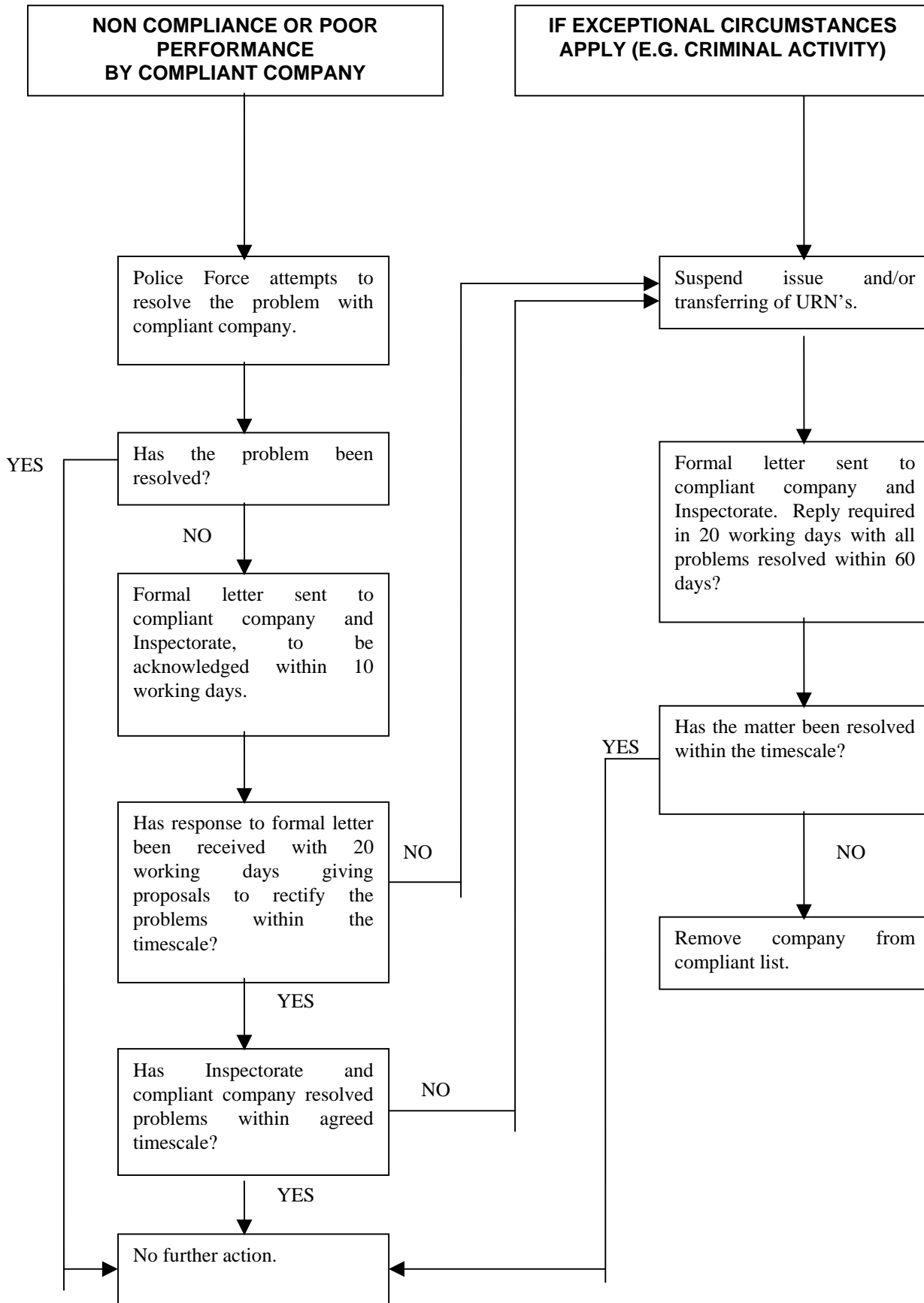
A properly installed security system will help to protect your premises when it is unoccupied. As you are considering the installation of a remote signalling security system you should be aware that the police have safeguards to reduce levels of false calls which divert us away from other tasks in your community.

To avoid misunderstanding, here is a précis of the conditions. However, should you require further information please contact your local Crime Prevention Officer.

1. Installation, maintenance and monitoring of security systems must only be undertaken by companies acceptable to your local police.
2. Such acceptance by the police does not imply guarantee of the company's work. You should seek confirmation from the company that it is compliant with police policy and is acceptable to the Police Force for the transmission of alarm messages from new installations.
3. You will receive training on the operation of the system by the installer including methods of cancelling accidental operations of the alarm.
4. Commercial premises may be required to have a 10 minute delay of sounders to give us the opportunity to attend and detain offenders. You may apply to Police Headquarters for exemption to the delay.
5. Any external audible sounder should cut out after 20 minutes and alarms causing annoyance under the terms of the Control of Pollution Act may result in prosecution. Some Local Authority areas may be subject of Section 9 of the Noise & Statutory Nuisance Act 1993, or in London The London Local Authorities Act 1991 (Misc Provisions) which places additional responsibilities on the occupier. Please check with the installing company, or your local Council for details.
6. Security systems will receive a police response determined by the nature of demand, priorities and resources which exist at the time. After 2 false calls in any 12 months you will be advised in writing so that you may take remedial action.
7. Following 3 false calls in any rolling 12 months, police attendance will be withdrawn. We will continue to attend personal attack alarms where these are identified separately by the alarm receiving centre provided the attack alarm does not generate a total of 2 false calls.
8. Police attendance may be restored if remedial action has been taken to rectify the fault, or when the system has achieved 3 months free of false calls. The application must be submitted by your security company, with supporting evidence. It is therefore in your interest to identify and correct the cause of any false alarm at the earliest opportunity.
9. On completion of the administration procedures your security company will be issued with a Unique Reference Number (URN) which identifies your system within our files to speed call handling. This number should be used in all correspondence to the police but please do not disclose it to any unauthorised person.
10. There is a requirement to have at least two keyholders, details of whom will be maintained by the Alarm Receiving Centre. Keyholders shall be trained to operate the security system, 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.
11. In accordance with the Data Protection Act 1998 personal information relating to you and your keyholders in connection with the security system may be held on a computer. Please ensure that relevant names and addresses are current.

It is regretted that such constraints are imposed but they are essential if we are to maintain the credibility of alarm systems, reduce false calls and provide you with an acceptable service.

MEMORANDUM OF UNDERSTANDING



APPENDIX R

REQUIREMENTS FOR COMPANIES INSTALLING AND MONITORING REMOTE CCTV SYSTEMS

1. INTRODUCTION

- 1.1 This document sets out the police requirements for remotely monitored detector activated CCTV systems to enable such systems to gain URNs from police forces.
- 1.2 Companies monitoring remotely monitored detector activated CCTV systems, known as RVRCs and Installers will ensure that these police requirements are brought to the attention of the users of such systems that require a police response.
- 1.3 Remotely monitored detector activated CCTV systems that are installed and monitored to the requirements stated in this policy, will be known as Type A systems and will be issued with a URN.
- 1.4 Systems for which police attendance may be required and which operate outside the procedures identified in the policy, will be known as Type B systems. URNs will not be issued to these systems.
- 1.5 The levels of police response to suspected crime reported by a Type A remotely monitored detector activated CCTV system, will be the same as that stated in the ACPO Security Systems Policy clause 3.1.

2. STANDARDS

- 2.1 Installers of remotely monitored detector activated CCTV systems will comply with all of the following standards and guidelines:
 - ACPO Security Systems Policy
 - BS 8418 Installation and remote monitoring of detector activated CCTV systems – Code of Practice
 - BS EN 50132-7: CCTV Application guidelines
- 2.2 RVRCs monitoring detector activated CCTV systems will conform to all of the following standards:
 - BS 5979 (Cat II):
 - BS 8418: Installation and remote monitoring of detector activated CCTV systems – Code of Practice

3. LEGAL REQUIREMENTS

- 3.1 Any remotely monitored detector activated CCTV system that requires police response will be installed and monitored in such a way as to ensure that any criminal activity recorded can be supported by correct operational procedures. It is recommended that all organisations draw up procedures to ensure compliance with the Data Protection Act 1998 and, where applicable, the Human Rights Act 1998.

4. PROCEDURES

- 4.1 The relevant police force will be sent a notice to install a remotely monitored detector activated CCTV system using Appendix F of the ACPO Security Systems Policy. A URN will be issued in line with the relevant police force policy (Appendix A of the ACPO Security Systems Policy refers).
- 4.2 The means of image collection and communication between the premises and the RVRC is a matter for the installer and the RVRC. However, the system will be installed to meet the requirements of Clause 2 of this appendix.

- 4.3 The system will be maintained in accordance with the BS 8418 Clause 13.1, and the requirements of the Data Protection Act 1998, CCTV Code of Practice (latest edition).
- 4.4 The system will have the capability of audio challenge, which is to be used if appropriate. Local environmental conditions will be taken into consideration.
- 4.5 The RVRC will only call the police if there is sufficient evidence in the images of unauthorised access to the site/premises and of actual criminal activity in progress.
- 4.6 The RVRC operator will provide sufficient location and criminal activity information to the police control room.
- 4.7 The RVRC will employ filtering techniques to avoid unnecessary calls being passed to the police.
- 4.8 Any images required by a police force for investigative purposes will be supplied upon request.
- 4.9 The RVRC will send the recorded evidence (or at least a working copy) in the first instance to the investigating officer, with a completed statement of evidence to show continuity.
- 4.10 RVRCs using digital recording methods will adhere to the procedures for processing digital images, issued jointly by the Home Office, ACPO and PSDB.

5. MANAGEMENT INFORMATION

- 5.1 RVRCs will provide management information that is compatible to ACPO in relationship with the systems for analysis.
- 5.2 The information supplied will give a detailed analysis of the total number of calls passed to the police, registered with the URN.
- 5.3 Remotely monitored detector activated CCTV systems will be subject to the same conditions as laid down in the ACPO Security Systems Policy (Clause 3 refers) for the relevant police forces in relation to the total number of incidents incorrectly passed to the police.
- 5.4 The Memorandum of Understanding (MOU) is applicable to CCTV systems.

6. INDEMNITY

- 6.1 This document does not impose any liability on any police force, its officers or the police authority arising out of the failure or timeliness in responding to an activation from a remotely monitored detector activated CCTV system.

REQUIREMENTS FOR SECURITY SYSTEM SERVICES

Association of Chief Police Officers (England, Wales and Northern Ireland) and The Association of British Insurers

Requirements for Security System Services

- I For the issue of a URN by police forces in England Wales and Northern Ireland, and/or to meet the minimum general recommendations for member companies of the Association of British Insurers, the installation / services provided by the Installation, Maintenance or Monitoring Company shall be certified in accordance with the provisions of this document by a certification body accredited to EN 45011 by United Kingdom Accreditation Service.
- II The Certification Body shall -
- a. Be a company limited by guarantee and not having a share capital. The company is to be formed in accordance with the relevant Companies Act identified in Annexe A.
 - b. Ensure the company law members/guarantors of the certification body shall be limited companies properly formed in accordance with the relevant Companies Acts identified in Annexe A or suitable individuals.
 - c. Ensure the memorandum and articles of association and their company law members/guarantors are specific to a certification body and identify the objects of a properly constituted certification body.
 - d. Provide audited accounts, where applicable, or such other accounts as are mandatory under Company Law, to show compliance with Clause 4.2(i) BS EN 45011: 1998
 - e. Carry out surveillance of certified service providers in accordance with the provisions of paragraph III. Surveillance shall be conducted at a minimum frequency of once per year and for installation companies, this surveillance shall include an inspection/functional test of installation(s) for compliance with the appropriate documents identified in Annexe A
 - f. Have documented procedures for the inspection and test of installed and maintained systems to ensure compliance with the appropriate documents identified in Appendix A.
 - g. Ensure personnel who have access to third party security arrangements as a result of this process shall be subject to a security vetting procedure to British Standard 7858 or an equivalent, which identifies any unspent convictions or associations, which may be deemed unacceptable.
 - h. Be required to establish if certification has been given and/or withdrawn by any other Certification Body accredited to this scheme when an Installation, Maintenance or Monitoring Company makes application for acceptance.
 - i. Where disciplinary action is pending, in process or has resulted in expulsion by Certification Body 'A' of an Installation, Maintenance or Monitoring Company, for non-compliance with documents identified in Appendix A, the non-compliance causing the disciplinary action must be resolved prior to approval by another Certification Body 'B'.
 - j. Deal with any complaint against an Installation, Maintenance or Monitoring Company made by a police force in England, Wales & Northern Ireland or member company of the Association of British Insurers (ABI), in accordance with the Memorandum of Understanding (Appendix J) identified in Annexe A.
 - k. Invite a member of the ACPO Security Systems Group and the ABI, to attend board meetings as an observer for agenda items relating to this scheme.

APPENDIX S (continued)

- I. Be invited to the ACPO Security Systems, Industry Liaison, Group Meetings and/or relevant meeting held by the ABI as and when deemed necessary by the Association.

III Installing, Maintaining and/or Monitoring Companies

The installing maintaining and/or monitoring company, commensurate with the services they provide, shall -

- a. Vet personnel who have access to third party security arrangements in accordance with British Standard 7858, which ensures personnel of good repute and identifies any unspent convictions or associations which may be deemed unacceptable.
- b. Have financial stability to trade, at present and in the future.
Guidance - The certification body in determining financial stability to trade, may consider checking bank references, court orders and annual accounts prepared by an independent accountant, i.e. as provided to the inland revenue. In the case of an incorporated company the audited annual accounts or such accounts as are statutorily required should a company be exempt from audit.
- c. Have adequate and relevant insurance in respect of employers, product, public, efficacy and wrongful advice liability.
Guidance - Insurance cover to a minimum of £1,000,000 per incident.
- d. Have competent management with responsibility for all services provided.
Guidance - Management must be conversant with the relevant standards for the services they provide and be competent to inspect and test systems. Their responsibility extends to services provided by sub-contractors who must comply with all aspects of this document.
- e. Have sufficient competent staff to carry out their contractual demands and the requirements of standards.
Guidance - The contractual demands and requirements of standards includes the design, planning, installation, system performance, operation, commissioning, false alarm management, complaint handling, maintenance and repair for security systems in accordance with the appropriate documents in Annexe A.
- f. Have adequate arrangements, documented procedures and systems in place for all of their activities.
Guidance - This covers all aspects of a companies installing, maintaining and monitoring activities and includes -
 - *Personnel (includes vetting, competence, qualification)*
 - *Sales (includes enquiry, survey, quotation, order)*
 - *Installation (includes design planning, commissioning, training of subscribers)*
 - *Maintenance (includes preventative and corrective)*
 - *System performance*
 - *Confidentiality*
 - *Handling of system activations, i.g. intruder alarm filtering*
 - *Complaint handling**The documented procedures are to the extent necessary to achieve consistency of application, in the case of NSI companies they will require a certificated quality management system.
Complaint handling needs to show logging, corrective action and review procedures.*
- g. Have suitable premises where confidentiality can be observed and with adequate safeguards for security of information on a 24 hour basis.
Guidance - Any means of electronic security protection used for this purpose shall comply with the minimum standards of these procedures. Alarm receiving centres and/or monitoring centres must comply with the appropriate standards in Annexe A.
- h. Have the necessary resources to support those activities.
Guidance - The necessary resources extends to all that are necessary to provide the services offered e.g. tools, test equipment, vehicles, office equipment, spares, personnel etc.
- i. Have sufficient systems installed and/or monitored to enable competence and trading history to be determined.

APPENDIX S (continued)

- j. Have immediate access to and comply with the standards and documents identified in Annexe A.
- k. Have customer contracts describing the products and services to be supplied together with the associated terms and conditions.
*They are to be fair and reasonable, describe the products and services to be provided, show title to any equipment, describe the terms of the warranty and detail **all** the charges applicable.*
- l. Not engage in pressurised selling or unfair business ethics.

IV New standards and documents applicable to this scheme will be notified by the Secretary to the ACPO Security Systems Group or the ABI to all Certification Bodies accredited to this scheme.

V Where amendments to this scheme are deemed appropriate by the Association of Chief Police Officers and/or the Association of British Insurers a consultation meeting will be instigated for attendance by those concerned.

ANNEXE A**British Standards and European Norms (Latest Issue)**

BS 4737	Intruder Alarms in Buildings
BS 7042	High Security
BS 8418	CCTV Systems
BS 5979 (Cat II)	Alarm Receiving Centres
BS 6799	Wire free Alarms
BS 7858	Vetting of Security Personnel
PD 6662	Scheme for the implementation of European Standards (Attention is drawn to BSIA Form 171 (Guidance Notes))
BS EN 50131-1	Alarm systems – Intrusion Systems – General requirements
BS EN 50131-6	Alarm Systems – Intrusion Systems – Power supplies
BS EN 50136-1-1	Alarm transmission systems – General Requirements
BS EN 50136-1-2	Alarm transmission systems – Requirements for systems using dedicated alarm paths
BS EN 50136-1-3	Alarm transmission systems – Requirements for systems with digital communicators using the public services telephone network
BS EN 50136-1-4	Alarm transmission systems – Requirements for systems with voice communications using the public services telephone network
BS EN 50132-7	Alarm systems – CCTV surveillance systems used in security applications – Application guidelines
BS 7939	Smoke Security Devices

British Standard Institute Drafts for Development (Latest Issue)

BS DD 242	High Security
BS DD 243	Automatic Re-Arming, Filtering and Substantiating Alarm Information
BS DD 244	Wire Free Alarms
BS DD 245	Management of False Alarms
DD CLC/TS 50131-7	Alarm Systems – Intrusion Systems – Application Guidelines

Legislation

The Environmental Protection Act 1990, The Control of Noise Order 1981 and the Clean Neighbourhood and Environment Act 2006 set out requirements for intruder alarms, keyholders and noise.

The Companies Act 1985 and 1989

Association of Chief Police Officers (England, Wales & Northern Ireland)
Security Systems Policy 2006

Memorandum of Understanding. (Dated: October 2005)

TEN POINT PLAN FOR PERSONAL ATTACK DEVICES**1) FILTERING**

The ARC's are not in a position to pass only confirmed PA's to the police. The fact that someone does not answer the telephone does not confirm the activation in genuine as access to the telephone may be restricted, or that staff are too busy to answer it. In the event of the telephone being answered an operator is not always in a position to determine from what is (or is not) heard, if the activation is genuine.

However, the ARC's are in a position to attempt to filter unwanted false activations, with intervention in place false calls will be reduced.

2) WITHDRAWAL OF POLICE RESPONSE

The Intruder Alarm part of a system will be allowed to receive the current amount of false calls before withdrawal of response. Police response will be withdrawn to the PA part of the system after a maximum of 2 false calls in a rolling 12 month period.

Where a system loses response to a PA, the security company should liaise with the end user to see if the PA element is necessary. If it is not required it should be removed.

Police response may be restored following receipt of evidence from the security company that the PA has been free of false calls for a period of 3 consecutive months.

Response may be reinstated to PA's before the 3 month period in the following circumstances:

- i) The security company must satisfy the police force concerned that a significant change has been made to that particular system to prevent further false calls. Reinstatement in this way can be obtained only once.
- ii) An additional form of confirmation has been installed to the system

3) PA DEVICES ON CIE OR ACE SHOULD BE SEGREGATED FROM THE MAIN KEYS, DEDICATED, DEFINED AND ARE 2 SEPARATE BUTTONS SYNCHRONISED PUSH.**4) PA DEVICES ON CIE OR ACE SHOULD BE ENGINEER PROGRAMMED ONLY (DEFAULT OFF)**

The implementation of this action will be dependant on the programming ability of the CIE or ACE. Re-engineering may be needed and therefore a lead time will be required. This will stop the PA signal being transmitted during watchdog failures or if the CIE reverts to default programming due to power problems.

5) DURESS CODES SHOULD ONLY BE ALLOWED FOR BS 7042 OR BS EN 50131-1 GRADE 4 SYSTEMS

The logic of restricting duress codes to high security systems to ensure that the risk warrants the facility. Inadvertent use of the duress codes from the CIE lead to a significant abuse of Police manpower.

6) DURESS FACILITY SHOULD BE ENGINEER PROGRAMMED ONLY (DEFAULT OFF)

The implementation of this action will be dependant on the programming ability of the CIE or ACE. Re-engineering may be needed and therefore a lead time will be required. The purpose of this software change is to ensure that the duress facility is restricted to BS 7042 and EN 50131 grade 4 systems and not customer programmable. This will stop the duress signal being transmitted during watchdog failures or if the CIE reverts to default programming due to power problems.

7) NO SINGLE ACTION 'SINGLE PUSH' PA DEVICES SHOULD BE ALLOWED

Only 2 separate buttons with synchronised push systems should be allowed, as this would stop accidental activation by people 'bumping' against the PA. Although this has been standard in the industry for many years, systems may need to be upgraded to 'double push' PA devices in the event of losing police response.

8) NO TIME DELAY DEVICES ARE TO BE ALLOWED

In these types of systems the PA is pressed once to start a timer. The occupier can then answer a door, check for intruders etc. If the PA is not pressed a second time, the timer will time out and the PA is sent. This type of arrangement is a recipe for false alarms and will need to be redesigned in the event of losing police response.

9) PORTABLE PA DEVICES (WIRELESS DEVICES) SHOULD BE DEDICATED AND NOT INCORPORATE ANY OTHER FUNCTIONALITY AND SHOULD HAVE 2 SEPARATE BUTTONS, SYNCHRONISE PUSH TO ACTIVATE

This requirement is to stop single button type PA's, eg care alarm type systems being used for PA's. Although this has been standard in the industry for many years, systems may need to be upgraded to 'double push' wireless devices in the event of losing police response.

10) TRAINING / RE-TRAINING OF USERS

The training or re-training of users should be incorporated into the maintenance. The user should also be made responsible for the training of their keyholder and this should be documented with the maintenance report.

Documentation should be provided to indicate when to use and when not to use a personal attack device. The keyholder should be made aware of the serious implications of misuse.

RACE & EQUALITY IMPACT ASSESSMENT

Assessment	Yes	No	Comments / Evidence
Does this Policy PROMOTE EQUALITY OF OPPORTUNITY?	✓		The Policy caters for the installation, maintenance, monitoring and police response to security systems. It is available for all persons regardless of race, age, religion, gender, disability or sexual orientation.
Does this Policy ELIMINATE RACIAL DISCRIMINATION?	✓		The Security Systems referred to in this Policy are mainly fitted or attached to premises both commercial and residential. Portable attack alarms are available to vulnerable people if required.
Does this Policy PROMOTE GOOD RACE RELATIONS BETWEEN PEOPLE FROM DIFFERENT GROUPS?	✓		The systems are available to any person or organisation.
Is there any evidence/belief that this Policy could affect some minority or ethnic groups differently?		✓	There is no evidence to suggest that this Policy could affect any groups differently.
Is there any public concern that this Policy is being carried out in a discriminatory way?		✓	The Policy has been in force since 1995 without any discriminatory issues ever being raised.

OVERALL IMPACT OF POLICY (HIGH, MEDIUM, LOW).....LOW.....

Name of person completing this Assessment: Mr K Meanwell
 Staff Officer
 ACPO Crime Prevention Initiatives Ltd

Date of Assessment: 14th October, 2005