

| | | | |
|------------------------------|----------------------------------|--------------------------------|---------------------|
| Security Classification: | | NOT PROTECTIVELY MARKED | |
| Disclosable under FOIA 2000: | | Yes | |
| Author: | Ken Meanwell | Force / Organisation: | ACPO CPI Ltd |
| Date Created: | 1st April 2012 | Telephone: | 01522 558377 |



**Association of Chief Police Officer of England,
Wales & Northern Ireland**

**Police Response to
Security Systems**

Status: This 'living' document is published by the Security Systems Working group within the General Policing Business Area and reviewed on a regular basis. **Having been reviewed this document is effective from 1st April 2012** It is disclosable under the Freedom of Information Act 2000, has been registered and audited in line with ACPO requirements (Appendix V) and is subject to Copyright.

**Implementation
Date:**

1st April 2012

Review Date:

Not more than one year

CONTENTS PAGE

| SECTION | Page No. |
|---------------------------------|-----------------|
| Preface | 3 |
| Guidance, Advice and Procedures | 3 - 6 |
| Operational Tactics | 6 - 9 |
| Learning Requirements | 9 - 10 |
| Appendices | 11 - 57 |

ACPO POLICY ON POLICE RESPONSE TO SECURITY SYSTEMS (April 2012)

1. PREFACE

- 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 / tracking centre (e.g. RVRC, SOC), 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. GUIDANCE, ADVICE AND PROCEDURES

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 security 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 2 and Type A requirements.

2.3. LIST OF COMPLIANT COMPANIES INSTALLING TYPE A SECURITY SYSTEMS

2.3.1 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.

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

- (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) Must apply and be 'Listed' with the home force where their main office/HQ is situated, before applying for inclusion on the list of other forces outside their main police force area.
- (d) 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.

2.4 Information to Customer

2.4.1 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**.

2.5 Notice to Customer Type A Systems

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

2.6 NOTICE TO INSTALL TYPE A SECURITY SYSTEM

2.6.1 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 **Appendices F** and **G**. (Only typed applications will be accepted).

2.6.2 All notices or other documents required for the issue or processing of a URN may be sent by electronic means or post.

2.6.3 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.

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

2.7 Variations

- 2.7.1 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**.

2.8 KEYHOLDERS

- 2.8.1 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 contactable by telephone, 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. Failure to comply with the above instructions could result in the URN being suspended.

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

- 2.8.3 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.

- 2.8.4. Requests for police response should only come from the ARC's, keyholders should not contact the police asking for their attendance.

2.9 DELAYS OF AUDIBLE SOUNDER AND ALARM ACTIVATED SECURITY DEVICES

- 2.9.1 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**)

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

2.10 FALSE ALARM MONITORING

- 2.10.1 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 installer's 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.

2.10.2 Definition – For the purpose of this policy, a false alarm is an alarm call (PA & Intruder) 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/lone worker/RMDA CCTV system made with good intent.
- d) Requests made by RVRCs for police to attend sightings of individual(s) seen on protected premises where no criminal activity, attempt/intent is in progress, will be considered as civil trespass and such calls would be classified as false.
- e) Activation of detectors without apparent damage or entry to the premises and line faults will be considered as a false alarm unless proved otherwise.

2.11. ADMINISTRATIVE CHARGES

2.11.1 Each application for a URN both Intruder and PA is subject to an administration fee payable by the system user. The URN fee is £43.49 plus VAT. Acceptable methods of payment (which may include BACS) and fee are identified within Appendix A and the ceiling will be reviewed by ACPO every year. The current policy on charging is set out in Appendix E. URNs for vehicle tracking and lone worker services are dealt with in Appendices U & V of this policy.

2.11.2 For intruder, PA and CCTV systems the installation/maintenance company will if requested satisfy an invoice from the police for the payment of the URN administration fee on behalf of the system user who shall always remain responsible for the fee. The fee shall be the amount set out in the current edition of the ACPO policy.

2.11.3 If the company satisfies an invoice referred to in 2.11.2, then the police and the company agree that this shall not constitute or imply any partnership, joint venture, agency, fiduciary or other relationship between either the company and the system user or the company and the police.

2.11.4 The fees for vehicle tracking and lone worker services will be reviewed by ACPO every year and may be different from the intruder, PA and CCTV system URN

2.12 MEMORANDUM OF UNDERSTANDING

2.12.1 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).

3 OPERATIONAL TACTICS

3.1 POLICE ATTENDANCE - Type A Security Systems

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

LEVEL 1 – Immediate/Urgent/Priority

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 Intruder and PA applications will only qualify for a URN and police response if installed to the current required standard (PD6662 scheme for application of European Standards for intruder and hold up alarm systems).
- 3.1.4 Intruder alarm systems (IAS) 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, not less than 14 days from the date of the Withdrawal letter. 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 PA/Hold Up alarm systems issued with a URN will receive LEVEL 1 response until two false calls have been received in a rolling 12 month period.
- 3.1.8 Following the first false call the customer may be advised in writing, with a copy being forwarded to the maintaining alarm company informing them of the situation and recommending urgent remedial action.
- 3.1.9 Following two false calls in 12 months LEVEL 3 will apply and police response will be withdrawn not less than 14 days from the date of withdrawal letter. 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.
- 3.1.10 Following withdrawal of response, the following conditions will apply in order to reinstate police response:
 - (i) Unconfirmed intruder and PA systems will need to be upgraded to a confirmed DD243:2004 or BS8243:2010 system with effect from 1st June 2012 (all systems installed prior to DD243 2002 are designated unconfirmed).
Reinstatement of police response may be achieved, without a 3 month delay, 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.
 - (ii) Confirmed DD243 (2002 / 2004) or BS8243:2010 systems will require the cause of the false alarms identified, remedial action

taken, or have an additional form of confirmation added or a period of 3 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.**

3.1.11 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. If the URN is for a combined system, only the element of the URN at level 3 will be deleted.

3.1.12 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) / Hold Up Alarms**

3.3.1 A deliberately operated device, known as a PA, may be operated to summon urgent police assistance when a person is threatened with immediate personal violence or criminal act. 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 and reinstatement of PA's must comply with the Ten Point Plan as specified in **Appendix T.**

3.3.3 For restoration of PA's which have lost response, confirmation is mandatory. Security Companies should apply for reinstatement using Appendix F Annexe B.

3.3.4 Where mandatory confirmation is required, it will remain in force for the life of that system.

3.3.5 In a system with both PA and intruder system, the remote signal shall differentiate between the two types.

3.3.6 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.

3.4 **POLICE ATTENDANCE - 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 and 3.4.3 above applies.

4. LEARNING REQUIREMENTS

4.1 Data Protection Act 1998

- 4.1.1 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.
- 4.1.2 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.

4.2 European Court of Human Rights Considerations

- 4.2.1 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.

4.3 Freedom of Information Act 2000

- 4.3.1 The Police Response to Security Systems Policy is publicly available and published on the ACPO Secured by Design website (www.securedbydesign.com via Professionals > Research & Publications > Publications).
- 4.3.2 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.

4.4 Racial Equality

- 4.4.1 The policy has been drafted taking into account the appropriate principles of the Equality Act 2010

4.5 Advertising

- 4.5.1 Installation Companies and ARC's 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 prior permission of the relevant chief officer of police.
- 4.5.2 The use of wording such as 'Police Approved', 'Police Preferred', 'Police Compliant' and 'Meets Police Requirements' must not be used.
- 4.5.3 Advertising material should not contain any references to recognised or compliant lists held by individual police forces. Photographic material or images of police officers or vehicles must not be used.

4.6 FINAL DISCRETION

- 4.6.1 The policy does not impose any liability on a police force, its officers or employees, the Police Authority or Police & Crime Commissioner arising out of any acts or omissions connected with the security system installation, including failure or timeliness in responding to any activations. 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.
- 4.6.2 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 Fire and Security Association (FSA) the insurance industry, represented by the RISC Authority and other representative organisations to review such matters.
- 4.6.3 The ACPO Police Response to Security Systems Policy is the copyright of the Association of Chief Police Officers. This Policy is available on the ACPO [Secured By Design](http://www.securedbydesign.com) website www.securedbydesign.com via Professionals > Research & Publications > Publications and may be downloaded for individual use, but under no circumstances altered or amended.
- 4.6.4 Other documents referred to in the policy (including the appendices) and communications on matters referred to in the policy must be in writing, facsimile or similar electronic form. Electronic copies of original documents and electronic documents shall be acceptable

5. INDEX TO APPENDICES

| | |
|--|---|
| APPENDIX A | POLICY VARIATIONS FORCE SERVICE STANDARD |
| APPENDIX B | APPLICATION FOR INCLUSION ON POLICE LIST OF COMPLIANT COMPANIES/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 ANNEXE B | RESTORATION OF RESPONSE TO INTRUDER ALARM 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 |
| <u>APPENDICES K-Q ARE ADVISORY STANDARD TEMPLATES, FOR USE BY FORCES, IF THEY SO REQUIRE.</u> | |
| APPENDIX K | <i>POLICE LETTER TO CUSTOMER ON COMPLETION OF INSTALLATION</i> |
| APPENDIX L | <i>NOTICE OF URN TO MAINTAINING COMPANY</i> |
| APPENDIX M | <i>LETTER TO SUBSCRIBER FOLLOWING 2 FALSE CALLS</i> |
| APPENDIX N | <i>LETTER TO SUBSCRIBER FOLLOWING 3 FALSE CALLS</i> |
| APPENDIX O | <i>REINSTATEMENT OF POLICE RESPONSE LETTER</i> |
| APPENDIX P | <i>DELETION OF URN/MONITORING LETTER TO SUBSCRIBER</i> |
| APPENDIX Q | <i>DELETION OF URN/MONITORING LETTER TO SECURITY SYSTEMS COMPANY</i> |
| APPENDIX R | REQUIREMENTS FOR COMPANIES INSTALLING AND MONITORING REMOTE CCTV SYSTEMS |
| APPENDIX S | REQUIREMENTS FOR SECURITY SYSTEMS SERVICES |
| APPENDIX T | TEN POINT PLAN FOR PERSONAL ATTACK DEVICES |
| APPENDIX U | REQUIREMENTS FOR ISSUE OF URNS FOR VEHICLE TRACKING |
| APPENDIX V | REQUIREMENTS OF LONE WORKER SERVICES |

POLICY VARIATIONS FORCE SERVICE STANDARD

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

Force Crest, Chief Officer's name and headquarters address

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

Examples

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 policy agreement (Appendix B).....(details of any annual fee/ premium rate charges).
3. ThePolice/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 security system companies must enclose a stamped addressed envelope with all correspondence requiring a reply.

All correspondence should be addressed to the Supervisor, Alarms Administration Department,address.

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

APPLICATION TO BE ACCEPTED ON POLICE LIST OF COMPLIANT COMPANIES /POLICY AGREEMENT FORM

APPENDIX B

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

You must be registered with your Home Force where your main office/headquarters is situated **before** applying to other police forces for inclusion on their List of Policy Compliant Security Companies.

Insert Name of Home Force registered with

I have read the (name of force) Police/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 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)

..... Position in Company

My company is inspected by..... for the following types of security systems

..... (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 Secured By Design website (www.securedbydesign.com).

Signature..... Print Full Name

Date.....

Address.....

.....Post Code.....

Telephone Number Fax Number.....

Email for correspondence.....

Email for Invoicing.....

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 (as amended by the Criminal Justice and Immigration Act 2008) applies and 'spent' convictions, reprimands, warnings, cautions and conditional cautions (adult and youth) 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, monitoring 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 area where the employee is based for work purposes. There should be no reason to carry out subsequent checks in other force areas.
- (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 meets/does not meet the criteria of the Policy.

APPENDIX C (continued)

- (viii) The police check will be limited to a PNC check against criminal convictions only. The police will reply stating the person meets/does not meet the criteria of this policy. Details of convictions will not be passed on to the employer.
- (ix) In the event of a pending prosecution where the offence is relevant, a decision on suitability may be delayed subject to the outcome of the case.
- (x) 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.
- (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. 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.
- (xii) In the event of a request for a police check from a foreign national, the application will also require an attachment of the relevant overseas criminal record check; this will need a form of authentication and be translated into English.
- (xiii) In the event of a British Citizen having worked outside of the UK for over a period of six continuous months in the last 5 years, they will also be required to provide an overseas criminal record check.

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 in assessing my suitability spent convictions and cautions are not considered by the police. I authorise the police to inform my employer if they consider I meet/do not meet the criteria of their Force Policy on Security Systems, because of any information obtained from police records. Where there is police bail or pending prosecutions the decision to notify your employer could be delayed for some considerable time.

Surname/Family Names

All First Names

Maiden/Former Names

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

Nationality.....

If born outside of the United Kingdom

Date of residency in UK.....

Position in company.....

Present Address

.....

.....

Previous Addresses in last 5 years (give dates):

.....

.....

(continue overleaf if necessary)

If you live overseas or you have spent six continuous months or more outside the UK, you must provide evidence of a criminal record check from the relevant country or countries. The checks need to cover the five years prior to this application.

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.

I confirm that Form B of Appendix C has been provided to the applicant.

I/We indemnify the Chief Officer of Police of (name of force.....) and all officers and police staff of the said police service against all actions, claims, costs and demands arising out of the giving of information in response to this request.

SIGNEDPRINT NAME.....

POSITION IN COMPANY.....

DATE

NAME AND ADDRESS OF COMPANY.....

.....

PART C - For Police use only

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

- No trace of convictions on details supplied.
- The subject appears identical with the person whose criminal record is attached.
- The subject does not meet the requirements of this policy

SIGNED DATE

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

THIS FORM AND THE CRIMINAL RECORD MUST BE RETAINED BY THE POLICE

APPENDIX C (continued)

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 meet/do not meet the requirements 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 may advise an employer/ prospective employer that an individual does not meet the requirements of the ACPO Policy, 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 (AS AMENDED BY THE CRIMINAL JUSTICE AND IMMIGRATION ACT 2008) 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

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

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 consumer's risk.

Producer's 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.

Consumer's 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 or element of a URN is subject to an administration fee payable by the system user. The URN Fee is £43.49 plus VAT and will be reviewed annually by ACPO. (See Appendices U & V for vehicle tracking and lone worker systems).
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 or other payment method fails to clear or is not honoured, the URN will be cancelled and the security system company informed.
3. The administration fee is payable for Intruder and PA applications and transfers for:
 - a) New URN applications
 - b) New occupiers/owners of premises taking over existing security systems (system retains false alarm history unless upgraded to DD243 2004 or BS 8243 2010)
 - c) Existing user changing security company (system retains false alarm history unless upgraded to DD243 2004 or BS8243)
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.
Where a security company applies to takeover a URN from an existing company and/or Maintenance Contract, they may do so supported by the customer's authority.
4. The administration fee is not applicable when:
 - a) A compliant security company acquires/purchases another compliant security company.
 - b) A security company ceases to trade and another company takes over the URNs within 28 days
 - c) Premises change name only (Evidence will be required to ensure it is a change of name only and not change of owner/user).
Systems will retain their false alarm history unless upgraded to DD243:2004 or BS8243.
5. In the event of police forces and security companies failing to reach an agreement in whether 3 or 4 above applies, ACPO Security Systems Group should be consulted who will make recommendations to Chief Constables.
6. In the event the installation does not proceed after the URN has been allocated, the fee is non-returnable
7. All security system monitoring centres operating under this policy must utilise the dedicated ex-directory lines nominated by each police force.
8. If caller line identification is operated, monitoring centres must not bar this facility on police calls.

APPENDIX E Cont'd

9. 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. Note: If the company pays the URN fee on behalf of the customer referred to above, then the police and the company agree that this shall not constitute or imply any partnership, joint venture, agency fiduciary or other relationship between either the company and system user or the company and the police.

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: |

DETAILS OF PROTECTED PREMISES

| | | | |
|---|---|-----------------------------|--|
| HOUSEHOLDER | Title: | Initial(s): | |
| | Surname: | | |
| | Business Name: | | |
| Trading/signage/building/ other Name | | | |
| Description of building | | | |
| 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: (Rural / new sites) | | | |

| |
|-----------------------|
| TYPE OF SYSTEM |
|-----------------------|

| |
|-----------------------------|
| TYPE OF CONFIRMATION |
|-----------------------------|

| |
|----------------------------|
| ADDITIONAL FEATURES |
|----------------------------|

| |
|------------------------|
| GRADE OF SYSTEM |
|------------------------|

| |
|------------------------------------|
| STANDARD TO WHICH INSTALLED |
|------------------------------------|

| | | | |
|-------------------------|--|--------------|--|
| EXISTING URN NO. | | | |
| Int | | CCTV | |
| PA | | Veh tracking | |

| |
|---|
| PREVIOUS USER (Company name when applicable) |
|---|

| | |
|------------------|----------------------|
| ADMIN FEE | SOUNDER DELAY |
|------------------|----------------------|

| | |
|---------------------------------|--|
| CERTIFICATE /Contract no | |
|---------------------------------|--|

Signed:
 Print Name:
 Position in company:
 Date:

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

POLICE USE ONLY

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) | Grade of System (1 2 3) |
|-------------------------------|---|--|------------------------------------|
| Intruder Alarm | Audio | None | Grade 2 |
| Personal Attack | Visual | Smoke Generator | Grade 3 |
| Combined IA/PA | Sequential | CCTV | Grade 4 |
| CCTV | Audio and Sequential | Lighting | |
| Vehicle tracking | Visual and Sequential | Chemical trace | |
| Lone Worker | Visual and Audio | Access control | |
| CAT 5 | Visual, Audio and Sequential | Smoke Raid Control (PA) | |

| ADMIN FEE (1 2 3) | STANDARD TO WHICH INSTALLED (1) | TYPE OF PREMISES (1) | VARIATION REASON(s) (1 2 3) |
|--------------------------|--|-----------------------------|--|
| Applicable | BS 4737 | Retail | Upgrade to confirmation |
| Not Applicable | PD6662 2004 + DD243 2004 | Commercial | Signalling amendment |
| | PD6662 2010 + BS8243 | Public Sector | New user |
| | BS 4737 + DD: 243:2002 | Licensed | Change of user name |
| | BS 4737 + DD243 2004 | Domestic | Address amendment |
| | BS 6799 Class VI | Industrial | Additional features |
| | BS 7042 | Bank or Financial | Takeover from another maintainer |
| | BS8418 2003 | Institutional | Change of Alarm Receiving Centre |
| | BS 8418 2010 | Other | Maintenance contract cancelled |
| | BS 8484 | | |
| | CAT 5 ATSVIVR | | 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**

Following the withdrawal of response letter the security company is required to apply for reinstatement using this form. Remedial work and/or re-certification of the system may be required as detailed below.

N.B. 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 | NAME & ADDRESS OF PREMISES | INSTALLER / MAINTAINER |
|-----|----------------------------|------------------------|
|-----|----------------------------|------------------------|

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

| CURRENT STATUS | REQUIREMENT | COMPLETED (✓) |
|--------------------------|----------------------------------|--------------------------|
| 1) Pre DD243 system | Upgrade to DD243:2004 or BS 8243 | <input type="checkbox"/> |
| 2) DD243 system pre 2002 | Upgrade to DD243:2004 or BS8243 | <input type="checkbox"/> |

Please note remedial action in 1 & 2 above could lead to reinstatement of response - without a 3 month delay.

| | | |
|----------------------|---|--------------------------|
| 3) DD243:2002 system | Identify cause, remedy, and detail remedial action in box below | <input type="checkbox"/> |
| 4) DD243:2004 system | Identify cause, remedy, and detail remedial action in box below | <input type="checkbox"/> |
| 5) PD6662 2010 | Identify cause, remedy and detail Remedial action in box below | <input type="checkbox"/> |

*Please note that systems in 3, 4 & 5 above must have been free of false calls for a continuous period of 3 months (supported by ARC evidence) **BEFORE** this application for restoration is submitted.*

There is no requirement to upgrade to PD6662 to regain police response

Identify the cause of the false alarms and give details of remedial work carried out in the box below (supported by evidence, such as an engineers report sheet)

Where a system has been upgraded a copy of the new NSI or SSAIB certificate of compliance/conformity must be forwarded with this application.

The information I have given is true to the best of my knowledge and belief. False or misleading information could lead to the loss of the URN

Signed:.....Name.....Date:.....

**Appendix F - ANNEXE B
April 2012**

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

Following the withdrawal of response letter the security company is required to apply for reinstatement using this form. Remedial work and/or re-certification of the system may be required as detailed below

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 | NAME & ADDRESS OF PREMISES | INSTALLER / MAINTAINER |
|-----|----------------------------|------------------------|
| | | |

1) Is a police response still required for the PA / Hold-up facility? **YES / NO**

If not, have appropriate measures been put in place to ensure that signals are not passed to the police? (the user may need to consult their insurance company, if the device has been removed). **YES / NO**

2) Confirmation is mandatory – is this in place? **YES**

3) **When a form of confirmation has been implemented for the first time, response may be reinstated to PA's before the 3 month period.**

Any subsequent Level 3 loss of response, after confirmation has been put place, a system must achieve three months' clear of false calls.

If the method of PA confirmation is not filtering out false calls effectively, the police reserve the right to request that one of the alternative methods are used

Where confirmation is mandatory to regain police response, an assessment must be carried out by the security company, to ensure that an appropriate confirmation method is used. In considering call back, audio or visual conformation, the purchasing contractor or other person responsible for health and safety under applicable legislation must ensure adequate support systems in place in the premises to ensure that no-one is placed at undue risk. Documentary evidence of this process must be retained by this person for inspection.

The method of confirmation used must be based on the security needs of the End User(s) and not for commercial reasons.

Please explain the method of confirmation used in this box, e.g. 'call-back', 'visual', 'audio', 'sequential' or 'any combination'.

4) Has the system been clear of false calls for three months? (If applicable*) **YES / NO**

5) Are all of the PA / Hold-up devices dual action? **YES**

Annexe B (continued)

6) Has the Duress facility been removed? **YES**
(Only PD6662 Grade 4 (Grade 3 in exceptional circumstances) & BS 7042 systems are exempt from this requirement. See Appendix 'T' (5).

7) Has user training been given? **YES**

8) Does PA/Hold-up alarm comply with all other aspects of Appendix T 10-point plan? **YES**

Give details of cause and any other work undertaken to rectify false PA alarms in this box.

I declare the End User(s) have been fully trained in the confirmation method and procedures to be followed in the event of the PA being activated.(A record of training is to be kept available for inspection by the police or inspectorate bodies).

The information I have given is true to the best of my knowledge and belief.

Signed:..... Date:.....

Name:.....(please print) Position in Company.....

Please note that false or deliberately misleading information provided on this form could lead to the loss of the URN.

HAZARDS AND SITE RISK STATEMENT (HEALTH & SAFETY) APPENDIX G
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 | |
| ATM <i>INSIDE PREMISES</i> | | SECURITY FOGGING DEVICE | |
| SMOKE RAID CONTROL (PA) | | | |

OTHERS:

| |
|--|
| |
|--|

IF NO SITE HAZARDS OR RISKS, STATE NONE:

| |
|--|
| |
|--|

The confirmed Following is

1. Alarm Receiving Centre has been given details of two keyholders capable of attending within 20 minutes of notification. The user is 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.
2. The system user irrevocably authorises the system installer/maintainer/security systems company, (the security company) at their own discretion to pay to the police the URN administration fee on his/her behalf and accepts, notwithstanding this, that the liability for the payment of the fee rests solely with the user, that the security company cannot be held liable in any way if it does not pay the fee and agrees to indemnify the security company against any financial liability incurred in connection with the payment of the URN fee.
3. The system user agrees that nothing in this or any other agreement shall constitute or imply any partnership, joint venture, agency, fiduciary relationship or other relationship between the parties or between the security company and the police.
4. The system user acknowledges that the payment of the URN administration fee does not imply any assurance that a URN will be provided by the police and the provision of a URN does not imply or guarantee any service or response from the police will be provided.

| | | | |
|----------------------------------|--|-----------------|--|
| Name of Occupier/Premises | | | |
| Address | | | |
| | | | |
| County | | Postcode | |
| Telephone Number | | | |

Signed:

| |
|--|
| |
|--|

 Print Name:

| |
|--|
| |
|--|

If commercial business;
 State position in Company:

| |
|--|
| |
|--|

 Date:

| |
|--|
| |
|--|

The POLICE ADMINISTRATION FEE (IF APPLICABLE) is £43.49 + VAT.

IF PAYMENT BY CHEQUE/POSTAL ORDER IS STILL REQUIRED BY FORCES, IT SHOULD BE MADE PAYABLE TO YOUR LOCAL FORCE POLICE AUTHORITY AND MUST BE ENCLOSED WITH THIS FORM AND RETURNED TO YOUR SECURITY SYSTEMS COMPANY.

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.

**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: 01628 637512

Fax: 01628 773367

E-mail: nsi@nsi.org.uk

Website: www.nsi.org.uk

SSAIB (Security Systems & Alarm Inspection Board)

7-11 Earsdon Road, West Monkseaton, Whitley Bay, Tyne & Wear. NE25 9SX

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 Listed 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. Many Traders who call at your door are honest and genuine, however, some are not and can be extremely persuasive. Examples of bad practices associated with cold-calling and door-step selling include - pressure selling, unclear contracts, over priced security systems and unduly raising the fear of crime. 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.

For further information on intruder alarm advice for domestic properties visit www.securedbydesign.com and www.consumerdirect.gov.uk/watch

APPENDIX I

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

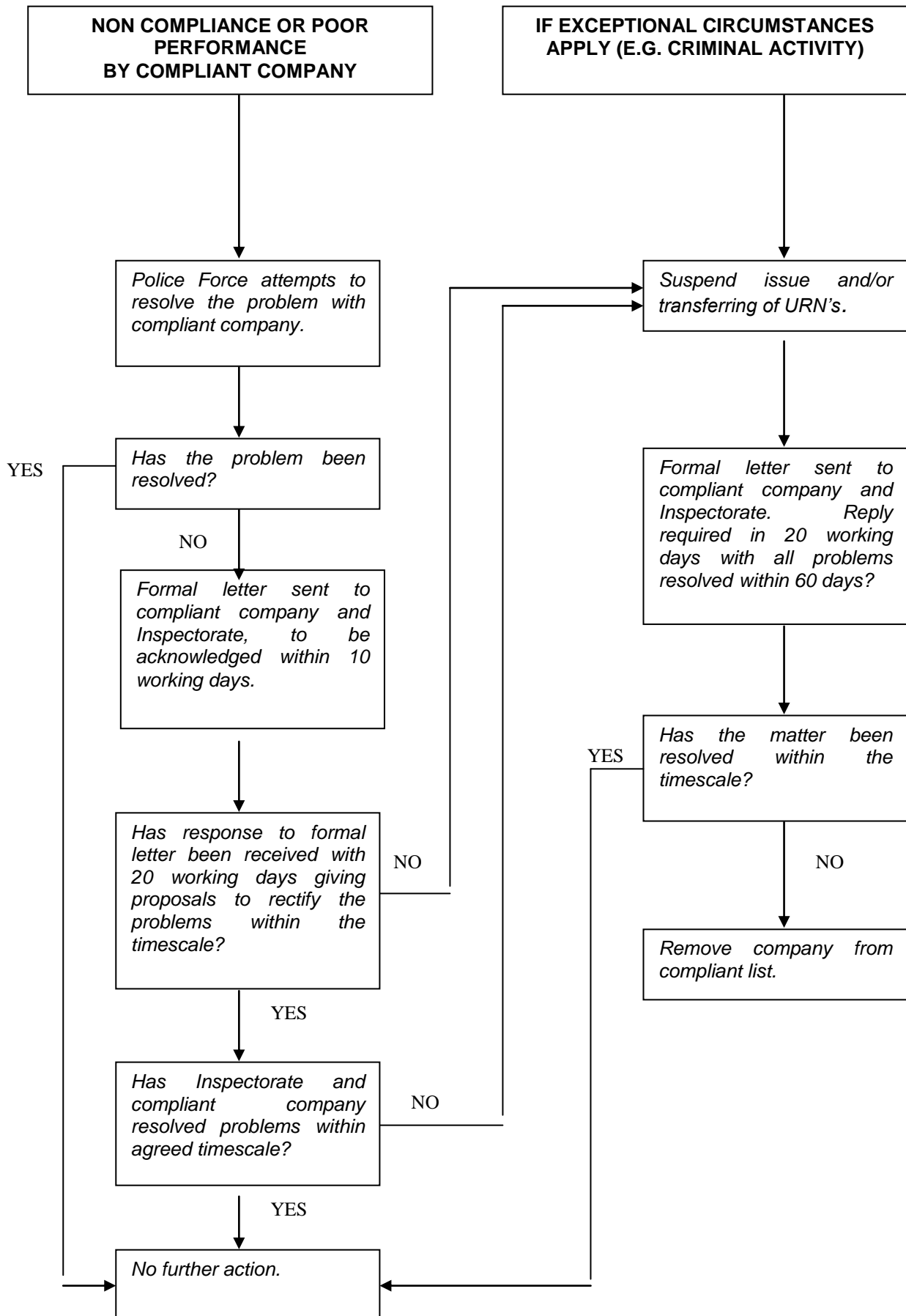
Dear Sir/Madam

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



POLICE LETTER TO CUSTOMER ON COMPLETION OF INSTALLATION

Dear Sir/Madam,

We are pleased to note that you are having a security system installed at your premises. Every possible attention is paid to calls emanating from such systems but in this connection we must seek your co-operation on the following important matters. Failure to comply with any of the following conditions may result in the police withdrawing response from your system.

You are advised that police personnel may have to be withdrawn from the premises before the arrival of a keyholder. In this case the keyholder may contact the police and ask them to re-attend if there is evidence of an offence.

1. FALSE ALARMS

Because of the considerable amount of time expended attending false calls, the Police have formulated the following policy:

Every user having a system which produces two false calls within a period of 12 months, shall be served with a notice requiring action to be taken to prevent further false calls.

Should three such calls be received within any 12 month period, police response will be withdrawn. Response may be reinstated if remedial action has been taken to rectify the fault, or when the system has achieved three months free of false calls.

Will you therefore please ensure that those involved in the operation of your security system are familiar with its functions and are informed of the importance of avoiding its accidental operation. Also, in the event of technical faults, please inform your system maintenance company as soon as possible after the fault has become apparent.

Ensure that the maintaining Alarm Company or the Alarm Receiving Centre is informed before commencement of any building or electrical work that may affect the operation of the intruder or hold-up system.

2. KEYHOLDERS

You should provide your alarm company with at least two keyholders for your premises. These keyholders shall be trained to operate the alarm, be contactable by telephone, have adequate means of transport to attend the premises at all hours, shall have access to all relevant parts of the premises and able to attend the premises within a 20 minute period.

3. NOISE NUISANCE

Your attention is also drawn to the Control of Noise Order 1981, The Environmental Protection Act 1990 and the Clean Neighbourhood and Environment Act 2006. This includes a 20 minute limit on the operation of audible warning devices.

4. PERSONAL ATTACK ALARMS

The Security Systems Policy states "A personal attack may be operated to summon urgent police assistance when a person is threatened with immediate personal violence or criminal act". However in many instances PAs are used where there is no threat to persons within a defined area. Without knowing the circumstances under which the PAs are activated, the police must respond. You should be aware that in the current policy, if you use the PA twice within in a rolling twelve month period and there is no threat to persons in a defined area, you will lose police response for a period of time.

Accidental misuse happens when staff are not trained in the use of a PA or visitors to the premises have access to the PA and press it out of curiosity. It is important that the PA is placed where members of the public cannot have access. Accidental misuse also occurs where duress codes are used. This is when a member of staff enters the duress code instead of the normal set or unset code. To prevent this happening all staff (including cleaning staff) who have access to the codes should be properly trained in the use of duress codes.

APPENDIX K (continued)

Accidental misuse of your PA system could cause you to lose police response. Guard against this possibility.

The following are examples of intentional but non-essential operation of a PA activation:

Garage forecourt attendant when someone has driven off without paying for petrol.
Shopkeeper because someone leaves the store without paying for goods.
Householder or publican who sees a fight in progress.
Householder who hears a suspicious noise outside

A PA is there to summon police assistance when you are threatened. DO NOT use it for any other purpose

5. DATA PROTECTION ACT 1998

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

Should you require further advice, please do not hesitate to contact this office.

Yours faithfully,

NOTICE OF URN TO INSTALLER

Dear Sir/Madam,

RE: _____

I acknowledge receipt of your recent Notice of Intention to Install a Security System at the above address.

Details of activations received at your Alarm Receiving Centre/Remote Video Response Centre should be passed to the _____ Police Force Call Handling Centre on _____. The message must include the Unique Reference Number _____ for use in the Call Handling Centre and failure to quote the URN will result in Police attendance being refused.

THE UNIQUE REFERENCE NUMBER MUST BE QUOTED IN ALL FUTURE CORRESPONDENCE RELATING TO THIS INSTALLATION.

It is a requirement of the _____ Police that all security systems installed should meet the British Standard BS EN 50131-1 (PD 6662 scheme for the implementation of European Standards), BS 4737, BS 7042, BS 6799 or BS 8418 and Codes of Practice identified in the Policy and that the installing company issue a certificate to that effect.

Re-setting of intruder alarm systems should be carried out only by a representative of your security systems company. Please note instant bells are permitted on residential premises/a ten minute bell delay will be required at this location/instant bells will be permitted at this location.

Yours faithfully,

LETTER TO BE FORWARDED TO SUBSCRIBER AT TWO FALSE CALLS

Dear Sir/Madam,

Security systems are only one example of the demand placed on the Police Service for an immediate response. False calls significantly outnumber genuine calls and divert police resources.

In an effort to reduce the unacceptably high number of false calls received by the Police, it has been necessary to introduce a policy governing the installation, maintenance, monitoring and use of security systems. The policy includes a close monitoring of all calls. Records indicate that there appears to have been at least two false calls from the system at your premises within a twelve-month period. In view of this, you are advised to contact your security systems company at the earliest opportunity in an effort to resolve what appears to be a problem with your security system or its operation.

Regrettably, should you have a total of three false calls within a rolling twelve month period, it will be necessary to consider the withdrawal of Police response to activations from your system, a situation we would wish to avoid with your co-operation.

You are advised to contact your Insurance Company and inform them of the contents of this letter as soon as possible as your insurance cover may be affected.

This information is brought to you with the assistance of your security company. Should you have any queries in respect of this letter, please contact your alarm company in the first instance, quoting your Unique Reference Number.

Yours faithfully,

Copy to: Security System Company

LETTER FROM POLICE TO CUSTOMER ADVISING WITHDRAWAL OF RESPONSE

Dear Sir/Madam,

I refer to previous correspondence concerning the operation of the security system at your premises.

Regretfully, continued monitoring of your security system has indicated that further false calls have been received.

Following careful consideration I have to inform you that Police response will no longer be given to your security system after the _____. Reinstatement of response can be considered following notification from your security company that your system has been upgraded if required, or remedial action has been taken to rectify the false calls and a period of three months free of false calls has been achieved. The action required will depend on which security system you currently have installed. Please contact your security company to clarify which option applies.

During the period of withdrawn response, your keyholder will continue to be informed of all activations by your monitoring station.

As the Police response is about to be withdrawn, I must point out that this action could affect any insurance cover you may have relating to the premises. You are therefore advised to contact your Insurance Company and advise them of the contents of this letter as soon as possible.

Yours faithfully,

Copy to: Security System Company

REINSTATEMENT OF POLICE RESPONSE LETTER

Dear Sir/Madam,

RE: _____

Further to your correspondence dated _____, the situation has now been reviewed.

I am able to inform you that police response to calls received from your security system at the above address has been reinstated to level 1 with immediate effect.

This decision however, must be made without prejudice on our part to again reducing response should a high incidence of false calls occur or should you fail to comply with the police Security Systems Policy.

I trust that the action you have taken will continue to be effective and may I thank you for your efforts in this matter.

Yours faithfully,

DELETION OF UNIQUE REFERENCE NUMBER – LETTER TO SUBSCRIBER

Dear Sir/Madam,

I refer to previous correspondence regarding the withdrawal of Police response from the above security system.

Response has remained withdrawn for a period in excess of 6 months and it has not been possible to reinstate response. Consequently a decision has been made to withdraw from monitoring the system with effect from the _____.

Your security system company has been instructed not to pass any further calls to the police after that date.

Advice regarding alternative means of security may be available from your local Crime Prevention Officer.

Yours faithfully,

DELETION OF UNIQUE REFERENCE NUMBER– LETTER TO SECURITY SYSTEM COMPANY

Dear Sir,

RE: _____

As a direct result of poor system performance, police response was withdrawn from the above system on the _____, and has remained withdrawn for a period in excess of six months.

Consequently, a decision has been made to withdraw the Unique Reference Number with effect from the _____.

After that time, further calls must not be passed to the Police. Your client is fully aware of the situation.

Yours faithfully,

**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 and the requirements of the Data Protection Act 1998, CCTV Code of Practice (latest edition).

APPENDIX R (continued)

- 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 there is criminal activity (or attempt) in progress, or the activity gives cause to suspect that there is intent to commit a crime.
- 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.

ASSOCIATION OF CHIEF POLICE OFFICERS (ENGLAND, WALES AND NORTHERN IRELAND)

Requirements for Security System Services

- I For the issue of a URN by police forces in England Wales and Northern Ireland, 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 Annexe 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 Annexe 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, in accordance with the Memorandum of Understanding (Appendix J).
 - k. Invite a member of the ACPO Security Systems Group 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 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. Trade lawfully
- 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 company's installing, maintaining and monitoring activities and includes -
Personnel (includes vetting, competence, qualification)
Sales (includes enquiry, survey, quotation, order)
Installation (includes design planning, commissioning, and training of subscribers)
Maintenance (includes preventative and corrective)
System performance
Confidentiality
Handling of system activations .e.g. intruder alarm filtering
Complaint handling
The documented procedures are to the extent necessary to achieve consistency of application.
Complaint handling needs to show logging, corrective action and review procedures.
- g. Have suitable premises where confidentiality can be maintained 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 all 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. Shall have sufficient business activity, relevant to the scope of this policy to enable competence and trading history to be determined by certification bodies.
- i. Have immediate access to and comply with 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 unlawful trading practices.

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

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

**British Standards and European Norms
(Current issue unless stated – see notes 1 & 2).**

| | |
|--------------------|---|
| BS 4737 | Intruder Alarms in Buildings (mostly withdrawn see note 2) |
| BS 7042 | High Security (withdrawn see note 2) |
| BS 8418 | Remotely monitored detector activated CCTV Systems |
| BS 5979 | Alarm Receiving Centres (Category II) |
| BS 6799 | Wire free Alarms (withdrawn see note 2) |
| BS 7858 | Security screening of individuals employed in a security environment |
| PD 6662:2010 | Scheme for the application of European Standards for intruder and hold- up Alarm systems. |
| PD 6662:2004 | Remains acceptable for new systems until 31 May 2012 (note 1) (Attention is drawn to BSIA Form 171 - Guidance Notes) |
| BS EN 50131 series | Intruder & Hold up Alarms |
| BS EN 50136 series | Alarm Transmission systems |
| BS EN 50131-8 | Smoke Security Devices (applies under PD6662:2010 – note 1) |
| BS 8473 | Management of False Alarms |
| BS 8243 | Installation & configuration of Intruder & HUAs designed to generate confirmed alarm systems (applies under PD6662:2010 – note 1) |
| BS8484 | Provision of Lone Worker Device Services |

British Standard Institution Drafts for Development (Latest Issue)

| | |
|-------------------------|---|
| BS DD 242 | High Security (withdrawn see note 2) |
| BS DD 243 | Applies under PD6662:2004 (note 1) |
| BS DD 244 | Wire Free Alarms (withdrawn see note 2) |
| BS DD263 | Alarms Systems Commissioning, Maintenance and remote support (applies Under PD6662:2010 see note 1) |
| DD CLC/TS 50131-7 :2008 | Alarm Systems – Intrusion Systems – Application Guidelines |
| DD CLC/TS 50131-7 :2003 | Applies under PD6662:2004 (note 1) |

Notes

1. Certain standards are in a period of “Dual running” with previous issues, and either current OR the previous issue may be acceptable for a specified, limited period.
2. Certain older and withdrawn standards or parts of standards are still included in this list for the benefit of legacy systems that remain in service.

Vehicle Tracking

Category 5 Criteria for System Operating Centres June 2010

Category 5 Criteria for original Equipment Manufacturers

ACPO & Centre for

Applied Science &

Technology (CAST)

HOSB 14/02 Stolen Vehicle Tracking and Remote Immobilisation Systems

CEN TS 15213 series Road transport & traffic telematics- After theft systems for recovery of stolen vehicles.

Legislation

The Clean Neighbourhood and Environment Act 2005 set out requirements for intruder alarms, keyholders and noise.

The Companies Act 1985 and 1989

TEN POINT PLAN FOR PERSONAL ATTACK/ HOLD UP ALARMS

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 is 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 confirmation 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.

When a form of confirmation has been implemented, police response may be reinstated to PA's before the 3 month period. Any subsequent loss of response, after confirmation has been put in place, a system must achieve three consecutive months free of false calls supported by evidence from the security company.

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.

Individual applications for duress facility may be considered for Grade 3 systems if the following requirements are complied with:

1. In premises that require high security, has duress been identified as an essential requirement from the risk assessment?
2. Is the duress notified separately from the hold up alarm signal?
3. Duress should not be initiated by using a digital key (fob).

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 (Grade 3 in exceptional circumstances) 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, e.g. 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.

REQUIREMENTS FOR COMPANIES INSTALLING AND MONITORING AFTER-THEFT SYSTEMS WITH VEHICLE IMMOBILISATION FOR VEHICLE RECOVERY

1. INTRODUCTION

- 1.1** This appendix sets out the police requirements for the installation and monitoring of After Theft Systems with Vehicle Immobilisation for Vehicle Recovery (ATSVIVR).
- 1.2** Only qualified and register personnel who meet these police requirements can install ATSVIVR systems.
- 1.3** Systems operating centre (SOC) who meet these police requirements can monitor ATSVIVR systems.
- 1.4** A SOC must agree and sign the ACPO and Industry approved indemnity letter and return this to each individual police force as part of the URN acceptance procedure.
- 1.5** A URN will be issued to a SOC for the purpose of monitoring ATSVIVR systems. This URN will be issued by each individual police force.
- 1.6** The police response to a reported ATSVIVR system which meets the requirements set out in this appendix will be level 1.
- 1.7** Other types of vehicle tracking systems that operate outside of this policy will be known as type B systems and a URN will not be issued to SOC to monitor such systems.
- 1.8** Any ARC's/SOC who have existing vehicle tracking contracts (known as legacy systems - these systems do not have Vehicle immobilisation) with the police may continue monitoring and reporting those existing systems. But these ARC's/SOC will not be issued with an ACPO URN.

2. AFSVRV REQUIREMENTS (See annex A of Appendix)

2.1 INSPECTORATE REQUIREMENTS

For an ATSVIVR system to be accepted by an SOC the installation service shall be inspected in accordance with the provision of this document by a certification body accredited to EN 45011 by the United Kingdom Accreditation Service. The exception to this is ATSVIVR systems fitted by the Original Equipment Manufacturer (OEM) at the car manufacturing plant.

For the SOC to be acceptable to ACPO it shall be inspected in accordance with the provisions of this document by a certification body accredited to EN 45011 with the scope of BS 5979CAT II and ISO 9001 by the United Kingdom Accreditation Service.

2.2 SYSTEM INSTALLATION REQUIREMENTS

- a. Installation shall be carried out by the car manufacturer at source or by a dealership or as an after market fit to the ATSVIVR manufacturers specifications.
- b. The after market fit shall only be undertaken by a company that is approved by an UKAS accredited inspectorate.
- c. The ATSVIVR system installed shall meet the installer requirements set down in the CEN TS 15213 series (*Road transport and traffic telematics – After-theft systems for the recovery of stolen vehicles*).

2.3 COMMISSIONING REQUIRMENTS

- a. The commissioning of the ATSVIVR will meet the requirements laid down in the Thatcham Category 5 Criteria for After Market and OEM for System Operating Centres (SOC) monitoring after theft systems for vehicle recovery.

- b. The commissioning shall be undertaken by organisations approved by Thatcham or a UKAS accredited inspectorate.

2.4 MONITORING (SOC) REQUIREMENTS

The requirements of the SOC are:

- a. BS 5979 Category II
- b. All personnel to be vetted to BS 7858
- c. SOC parts of the CEN/TS 15213 Series
- d. CAST 14/02 – stolen vehicles
- e. BS ISO 9001:2000
- f. Category 5 Criteria as listed in Appendix S

3. LEGAL REQUIREMENTS

All documentation and data pertaining to personal data of the owner of the vehicle with an AFSVIVR system installed shall be processed as per the Data Protection Act 1998.

4. POLICE ATTENDANCE

- a. For ATSVIVR systems police attendance will be a level 1 – Immediate/ urgent.
- b. If a single customer has 3 false alarm calls in a rolling 12 month period the SOC will remove that customer from police response until the customer can prove that the fault/procedure failures that caused the false alarms has been corrected. If the customer continues to have false alarms the customer will lose police response for 3 months and will only be reconnected if the 3-month period is free from false alarms.
- c. No SOC URN can be withdrawn from by an individual police force, but individual police forces can request through ACPO that the MoU is implemented on a poor performing SOC

5. PROCEDURES

- 5.1** When a vehicle is stolen the vehicle owner shall contact their local police and report the incident and obtain a crime Reference number (CRN).
- 5.2** The vehicle owner shall then contact the SOC and report the stolen vehicle and give the SOC the CRN.
- 5.3** The SOC will then locate the stolen vehicle and contact the relevant police force.
- 5.4** The SOC will keep in touch with the relevant police force directing the police to the location of the stolen vehicle.
- 5.5** The SOC shall keep monitoring the location of the stolen vehicle until informed otherwise by the police.
- 5.6** If required the SOC will activate the stolen vehicle's "immobilisations" device. It is important to note that the order to activate the vehicle's immobilisation device can only be given by a police officer who has the stolen vehicle in their line of sight.

6. MANAGEMENT INFORMATION

- 6.1** The SOC will ensure that they have a false alarm management system in place.
- 6.2** The SOC shall hold alarm statistics on all their customers and when required provide to ACPO relevant system management statistics.
- 6.3** The SOC will inform customers who have repeated false alarms that they may lose police response if the cause of the false alarm is not remedied. The SOC will keep statistics on such cases.

7. URN REQUIREMENTS

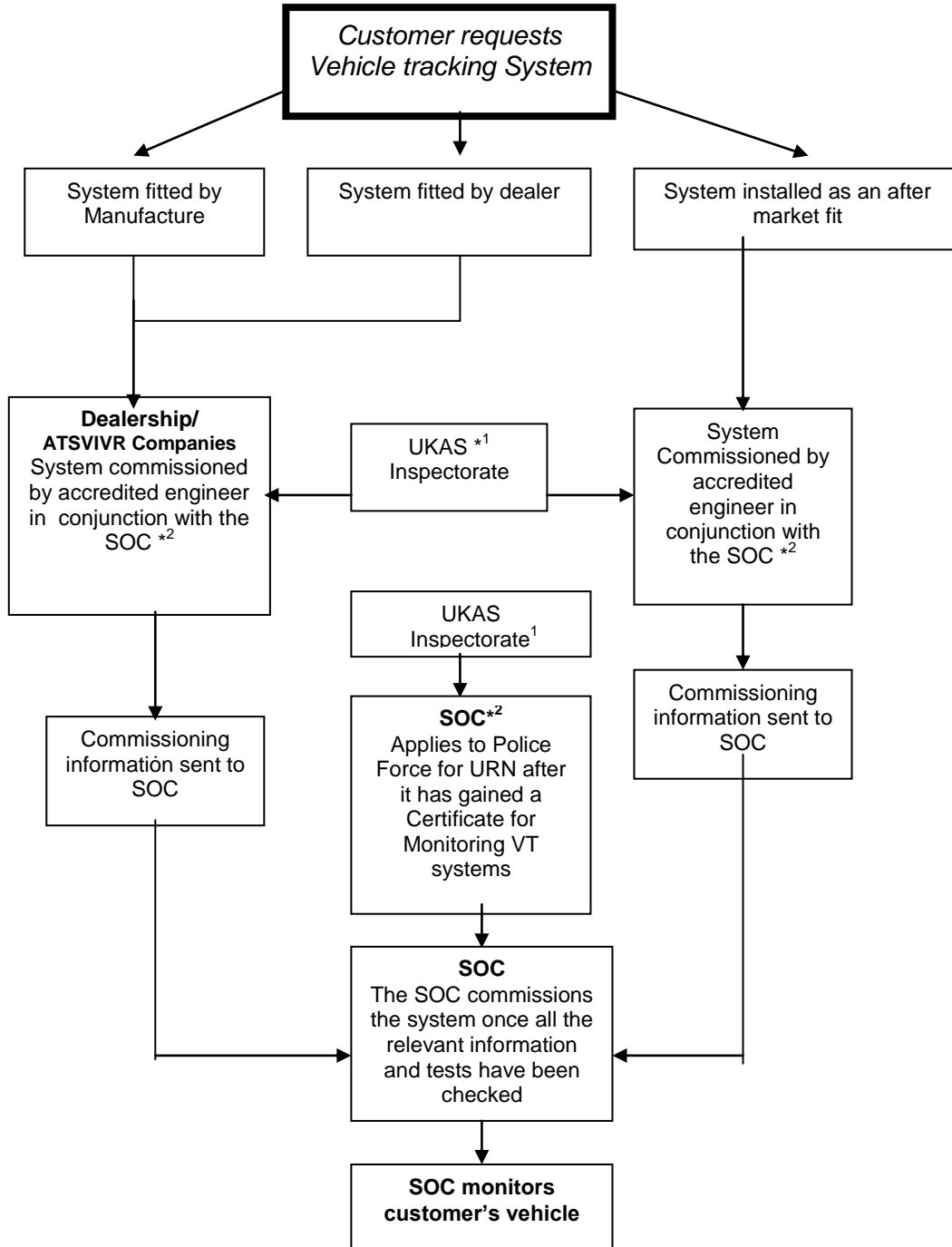
7.1 The SOC will apply to the relevant police force area for a URN. The cost of the URN will be £52.55 plus VAT Renewable on the 1st April per annum..

7.2 The SOC is to apply to the Chief Office r of Police for a URN using Appendix F of this policy.

8. INDEMNITY

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 activation from an ATSVIVR system.

ACPO VEHICLE TRACKING REQUIREMENTS FOR THE ALLOCATION OF A URN FOR A THATCHAM CATEGORY 5 SYSTEM WITH VEHICLE IMMOBILISATION CAPABILITY



Notes:

- *1 Accredited engineer shall be vetted (BS 7858 and have a police or CRB check).
- *2 The SOC is to submit the approved indemnity letter to Police forces.

AFTER THEFT VEHICLE IMMOBILISATION SYSTEMS INDEMNITY
DOCUMENT FOR SYSTEM OPERATING CENTRE

To: Chief Constable:.....(Name of Force).

From

Date

Reference HOSBD 14/02 – STOLEN VEHICLE TRACKING ACPO AND HOME
OFFICE GUIDANCE TO COMPANIES ON POLICE POLICY
(including After Theft Vehicle Immobilisation Systems)

The SOC operated by (**Name of Company**) is willing to indemnify you as stated in
The HOSBD 14/02 Clause 9.1 which states:

“Vehicle tracking and locator companies will indemnify, in writing, each chief constable where it is intended that the system will operate. The indemnity shall cover Police Authorities, their officers and servants, the chief constable and all members of the police service, against any claim under any course of action made by any person

- a) in respect of any loss, damage, expense, personal injury (including death), wrongful arrest, prosecution or charge caused by the negligent operation of the system by the company, or by any malfunction of the system which results in a vehicle being wrongly identified as stolen.”

It is important to note that the SOC will only operate the After Theft Vehicle Immobilisation System once they have been requested to do so by a police officer whose identity has been confirmed and who is in visual contact with the stolen vehicle and who has confirmed to the SOC that the stolen vehicle is parked in a safe place.

The SOC will not indemnify against:

- a. The failure of the vehicle immobilisation system (hardware/software) once the command has been sent.
- b. The failure of the communication network outside of the SOC control to send the signal to the target vehicle.
- c. Any failure due to faulty immobilisation system installation into the vehicle.
- d. Any delay of the activation of the immobilisation system, after the SOC has dispatched the signal, due to the geographical location of the vehicle and the time the network uses to transmit the signal from the SOC to the vehicle.

- e. Any incident that occurs after the SOC has been requested by a police officer to activate the vehicle immobilising signal and the successful Activation of the immobilising device.

The SOC believes that the above liability requirements places responsibility for

ANNEXE B CONT'D

liability on the SOC on the area that the SOC has control of and no other areas.

The SOC believes that the use of HOSBD 14/02 and the use of vehicle immobilisation systems will be a service of benefit to the police service and that through a partnership approach can contribute to the reduction of vehicle crime in the UK.

Signature _____

Name of Person _____

Job Title _____

Date _____

POLICE REQUIREMENTS FOR LONE WORKER SERVICES

1. INTRODUCTION

- 1.1 This appendix sets out the police requirements for the provision of lone worker services requiring police response.
- 1.2 ARCs who meet these police requirements will be able to apply for a URN to gain police response for lone worker systems.
- 1.3 Alarm Receiving Centres shall have filtering and verification processes in place to cut out any false alarms from LWDs and the police shall only be called in situations where a police response is required. In non-threat situations other types of response from other agencies or supervisors may be required. In these circumstances the police should not be called otherwise it may count as a false activation.
- 1.4 The supplier shall inform the customer of the requirements of the ACPO Security Systems Policy including this Appendix.
- 1.5 The customer shall be trained by the supplier to use the LWD and also how to cancel any false activations that occur so as to minimise any false calls.

2 URN REQUIREMENTS

- 2.1 The ARC will apply to the relevant police force for a URN. The cost of the URN will depend on The number of devices monitored nationally:
 - Under 10,000 £52.55 plus VAT per annum.
 - 10,000 – 50,000 £78.82 plus VAT per annum.
 - 50,000 or above £105.10 plus VAT per annum.Renewable on 1st April per annum.
- 2.2 The ARC is to apply to the Chief Officer of Police for a URN using the Appendix F of this policy.

3 FALSE ALARMS

- 3.1 The amount of false alarms as stated in clause 3.1.5 of the main ACPO Security Systems Policy does not apply to lone worker systems.
- 3.2 Police forces will monitor the number of false alarms per URN and supply these numbers to the ACPO security Systems Group Secretariat at the end of each calendar month.

4 DEVICE REQUIREMENTS

4.1 Lone Worker Devices shall:

- a. Meet the lone worker device requirements laid down in BS 8484:2009

4.2 Lone Worker Suppliers shall:

- a. Meet the Lone Worker supplier requirements laid down in BS 8484
- b. Meet the requirements as laid down in Appendix S, sub clause III, except sub clause 'I'
- c. The supplier shall be certified by a United Kingdom Accreditation Service (UKAS) accredited certification body to the provisions of the ACPO policy document "Police response to Security Systems".

5 MONITORING (ARC) REQUIREMENTS

5.1 The ARC shall:

- a. Meet the ARC requirements laid down in BS 8484:2009
- b. Conform to BS 5979 Cat 11
- c. The ARC shall be certified by a United Kingdom Accreditation Service (UKAS) accredited certification body in accordance with the provisions of the ACPO requirements for lone worker systems.

6 LEGAL REQUIREMENTS

All the documentation and data pertaining to personal data with respect to Lone Worker Services shall be processed in accordance with the Data Protection Act 1998.

7 POLICE ATTENDANCE

- 7.1 Lone Worker services which meet the requirements of the ACPO Security Systems Policy will receive a LEVEL 1 – Immediate/Urgent/Priority police response, (see 3.1.1 of policy).
- 7.2 If police response is withdrawn it will be for a period of 3 months, or until the customer can prove to the relevant police force that the cause of the false alarms has been corrected.
- 7.3 Police response will not be withdrawn by individual police forces without prior consultation with the ACPO Security Systems Secretariat.

8 PROCEDURES

- 8.1 When a LWD is activated the ARC shall carry out the procedures set down in BS 8484:2009 and those set down in the response agreement, (note the response agreement does not supersede these

ACPO requirements).

- 8.2 The ARC operator is to determine the nature of the incident from audio information received and where safe to do so, contact the lone worker either by 2 way radio or other means to find out more about the incident to ensure the correct level of response is attained and that the police are not called to a non emergency response.
- 8.3 Once the ARC operator has determined that the incident does require an emergency police response the ARC operator is to contact the police giving as much information about the incident as possible including the lone worker details and any information about other responders dispatched to the incident.
- 8.4 The ARC operator is to update the police control room on any changes to the incident or lone worker location whilst the police are attending the incident.
- 8.5 The ARC operator shall monitor the incident until informed otherwise by the police. The audio recordings of the incident may be required for police investigation and/or evidential purposes and should be managed as per the Data Protection Act.

9 MANAGEMENT INFORMATION

- 9.1 The ARC and the supplier shall ensure that they have a false alarm management system in place.
- 9.2 The ARC shall hold statistics on all their customers and when required provide ACPO with relevant data
- 9.3 The ARC shall inform the customer when false alarms occur and when the customer is about to lose police response

10 INDEMNITY

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 lone worker system, or the failure to locate the lone worker if the location information is not accurate.