Avon and Somerset Constabulary

Policy Statements

Communications Support Unit

Security Marking: **Not Protectively Marked**

ACPO Security Systems

(Unique Ref Number: 52QP-1161-08)

1. We will adopt the ACPO Security Systems Policy April 2008 with the following amendments to take account of local practice:

   a. Appendix A sets out the variations permitted in the Policy that this Force will take into use.

   b. Appendix D: The formula published by the ACPO Security Systems Group will not be utilised.

   c. Appendices K – Q of the ACPO policy will not be adopted by Avon and Somerset Constabulary.

2. We are committed to building a safer community by striving to maximise available resources. In order to achieve this, the Constabulary encourages partnership approach in providing the highest possible standard of service by reducing the number of false alarm calls.

Relevant legislation:

Human Rights Act 1998
Police Act 1996
Police and Criminal Evidence Act 1984
Common Law
Private Security Industry Act 2001

Related References:

ACPO Security Systems Procedural Guidance

How to complain about this policy:

Complaints about this policy may be made via:
Police Misconduct and Complaints against Members of Staff
Direction and Control Complaints (not yet available)

Introduction

Avon and Somerset Constabulary has adopted the ACPO Security Systems Policy 2009.

Procedural Guidance Information	
Policy Statement Owner:	Alarms Officer, Communications Support
Date Reviewed for Human Rights Compliance:	Okechukwu Adieze, 18-11-04
Effective Commencement Date:	02/05/06
Last Review Completed:	April 2009
Next Review Due:	April 2010

Security Classification:		**NOT PROTECTIVELY MARKED**	
Disclosable under FOIA 2000:		**Yes**	
Author:	**Ken Meanwell**	Force / Organisation:	**ACPO CPI Ltd**
Date Created:	**April 2009**	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 April 2009.** 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: April 2009

Review Date: Not more than one year

C O N T E N T S P A G E

SECTION	Page No.
Preface	3
Guidance, Advice and Procedures	3 - 6
Operational Tactics	6 – 8
Learning Requirements	8 - 9
Appendices	10 - 47

Copyright © 2003. All rights reserved. Association of Chief Police Officers of England, Wales and Northern Ireland. Registered number: 344583: 10 Victoria Street, London. SW1H 0NN.

ACPO POLICY ON POLICE RESPONSE TO SECURITY SYSTEMS (April 2009)

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 **Appendix F**.

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

2.6.3 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.

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.

2.9 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 installers inspectorate body as set out at **Appendix D**. The Force may determine whether the formula will be based on police statistics or on those supplied by the company.

2.10.2 Definition – For the purpose of this policy, a false alarm is an alarm call which would normally be passed to the police and has not resulted from:

a) a criminal attack, or attempts at such, on the protected premises, the alarm equipment or the line carrying the alarm signal.
b) actions by the emergency services in the execution of their duty.
c) a call emanating from a personal attack system made with good intent.

d) Requests made by RVRCs for police to attend sightings of individual(s) seen on protected premises where no criminal activity 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 is subject to an administration fee payable by the system user. The URN fee is £41.38 plus VAT. Acceptable methods of payment and fee are identified within Appendix A and the ceiling will be reviewed by ACPO every two years. The current policy on charging is set out in Appendix E.

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

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

LEVEL 1 – Immediate/Urgent
It should be noted that police response is ultimately determined by the nature of demand, priorities and resources which exist at the time a request for police response is received.

LEVEL 3 – Withdrawn
No Police attendance, keyholder response only.

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

3.1.4 All new 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).

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

3.1.6 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.

3.1.7 Following three false calls in 12 months LEVEL 3 will apply and police response will be withdrawn, not less than fourteen 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.

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

(i) Unconfirmed systems will need to be upgraded to a confirmed DD243 (2004) system (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) systems will require the cause of the false alarms identified, remedial action taken and 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.**

3.1.9 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, both the intruder and hold-up devices will be deleted.

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

3.2 **CCTV Systems**

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

3.3 **Personal attack alarms (PA).**

3.3.1 A deliberately operated device, known as a PA, may be operated to summon urgent police assistance when 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, Intervention is mandatory. Security Companies should apply for reinstatement using Appendix F Annexe B.

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

3.3.5 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 above apply.

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 > Guides & 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 Sections 2 (2) and (3) of the Race Relations Act (Statutory Duties) Order 2001.

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 or the Police Authority arising out of any acts or omissions connected with the security system installation, including failure or timeliness in responding to any 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 Insurance Property Crime Research Committee (IPCRes) 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 website www.securedbydesign.com via Professionals > Guides & Publications > Publications and may be downloaded for individual use, but under no circumstances altered or amended.

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	RESTORATION OF RESPONSE TO INTRUDER ALARM
ANNEXE B	RESTORATION OF RESPONSE TO PA ALARM
APPENDIX G	HAZARDS AND SITE RISK STATEMENT (HEALTH & SAFETY)
APPENDIX H	POLICY COMPLIANT COMPANIES – POLICE ADVICE TO PUBLIC
APPENDIX I	LETTER TO POTENTIAL CUSTOMER
APPENDIX J	MEMORANDUM OF UNDERSTANDING

APPENDICES K-Q ARE ADVISORY STANDARD TEMPLATES, FOR USE BY FORCES, IF THEY SO REQUIRE.

APPENDIX K	*POLICE LETTER TO CUSTOMER ON COMPLETION OF INSTALLATION*
APPENDIX L	*NOTICE OF URN TO MAINTAINING COMPANY*
APPENDIX M	*LETTER TO SUBSCRIBER FOLLOWING 2 FALSE CALLS*
APPENDIX N	*LETTER TO SUBSCRIBER FOLLOWING 3 FALSE CALLS*
APPENDIX O	*REINSTATEMENT OF POLICE RESPONSE LETTER*
APPENDIX P	*DELETION OF URN/MONITORING LETTER TO SUBSCRIBER*
APPENDIX Q	*DELETION OF URN/MONITORING LETTER TO SECURITY SYSTEMS COMPANY*
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 A

ACPO Security Systems Policy (April 2009)
Appendix A (Local Procedures)

The Avon and Somerset Constabulary has adopted the ACPO Security Systems Policy 2008. The following information and local requirements apply in this force area and are permitted under the terms of the policy.

1. SERVICE STANDARD

The Avon and Somerset Constabulary service standard is to aim to attend all immediate calls within 15 minutes in urban areas and 20 minutes in rural areas. This applies to confirmed, personal attack and duress calls. All other calls from security systems are graded as prompt. The force aims to attend all prompt calls within 30 minutes.

2. PASSING OF CALLS TO POLICE CONTROL CENTRES

All calls from security systems passed to this force must be directed to the Control Centre utilising the designated telephone number. Please note that all alarm activations must be reported using the correct police URN issued by us in writing to you and your client. Avon and Somerset Constabulary will not accept a call when the alarm customer's name and/or address differ from the Police record. You must therefore update us, using the appropriate police appendix, whenever this information changes. Details of the Control Centre telephone number will only be disclosed to policy compliant alarm receiving centres and system monitoring centres.

3. ADMINISTRATION CHARGES

The current URN fee is £44.05 (including VAT @ 15%) As from 1st April 2009 the administration charge for the issue of a URN will be £41.38 + VAT @ 15% = **£47.58** in total. Payment for this amount must be forwarded with each URN application. Acceptable methods of payment include Cheque or Postal Order. Please send one cheque / postal order per application. Cheques etc must be made payable to The Avon and Somerset Constabulary. See Appendix E for further information.

4. WARNING LETTERS AND NOTICES OF WITHDRAWAL OF RESPONSE

will be generated by the Force Alarms Officer and forwarded directly to the system user. Copies of such correspondence will be sent to the relevant security company. Following the issue of a warning letter and a 3 month period free of false calls, resumption of level 1 response will be automatic. No correspondence is therefore necessary.

5. DELAYS OF AUDIBLE/VISUAL WARNINGS

There is no requirement for audible/visual warning devices to be delayed following an activation. If a delay is incorporated in a system for any reason (e.g. audio confirmation) the delay must be declared.

6. CONNECTIONS TO POLICE CONTROL CENTRES

Security system signalling terminating in Police Control Centres is not permitted.

7. KEY HOLDERS
Key holder records are still maintained by this Force. Details of key holders complying with the criteria in Section 2.8 must be supplied with URN applications.

8. DISCLOSURE OF CONVICTIONS
Disclosure of Convictions applies to all compliant companies with an installing branch within the Avon and Somerset Constabulary area. With the exception of National Companies with regional branches, security checks for companies outside of this force area will not be undertaken. All Appendix C Convictions checks are to be forwarded to 'The Force Alarms Officer' at the address below.

9. FORCE WEBSITE
A copy of our policy is available on the Force website at www.avonandsomerset.police.uk and may be downloaded for individual, company or organisational use.

10. USE OF STANDARD FORMS
All Application, amendments and cancellation of alarm records are to be submitted on the standard forms in Appendix F. All Hazard forms submitted with new applications are to be on the standard form in Appendix G. Applications for restoration of Police response to Intruder and Personal Attack/Hold up Alarms are to be submitted on the appropriate forms in Appendix F, Annex A & B.

11. URN AUDITS
The Avon and Somerset Constabulary Alarms Administration Office will carry out an Audit of all URN's periodically. A list of URN records will be required on request from each compliantsecurity company. This will ensure compliance with the Data Protection and Freedom of Information Act.

12. CORRESPONDENCE
The Unique Reference Number (URN) must be quoted in all correspondence concerning security systems. In the interests of maintaining security, enquiries concerning security systems should be made in writing. Telephone enquiries regarding systems or activations may not be accepted.

All mail correspondence should be addressed to:-
The Force Alarms Officer
Communications Support Unit
Avon & Somerset Constabulary
PO Box 37
Valley Road
Portishead
Bristol
BS20 8QJ

A stamped addressed envelope will be required for each application or letter requiring a response.

All email correspondence should be addressed to:-
Alarms.office@avonandsomerset.police.uk

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

This appendix is available as a separate download from the website in Word format.

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.

(vi) Employers must make every effort to confirm the identity of the applicant before the police are required to process the check. They must also confirm the correct spelling of the full name, the date and place of birth and current address.

(vii) All applicants must give written permission for the police to instigate checks and also advise employers where they consider an applicant unsuitable within the terms of the Policy.

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 12 months in the last 3 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 me to be an unsuitable employee under 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

Position in company.....

Present Address .....

.....

.....

Previous Addresses in last 5 years (give dates):

.....

.....

.....
(continue overleaf if necessary)

Have you ever been convicted at a Court for any offence which is not now spent under the terms of the Rehabilitation of Offenders Act 1974? YES/NO
Are you about to be or are currently the subject of a pending court case? YES/NO
Are you currently on police bail YES/NO
I agree to notify my employer of any future relevant convictions
If YES, provide details overleaf, including approximate date, the offence, and the Court or Police Force which dealt with you.

Signature ..... Date .....

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.

SIGNED ……PRINT 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.
❍❑❑❑❑❑❑❑❑❑❑or

●❑❑❑❑❑❑❑❑❑❑&
☒ ☒ The subject appears identical with the person
☒ ☒ whose criminal record is attached.
❍❑❑❑❑❑❑❑❑❑❑or

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 are considered to be unsuitable for employment under the terms of their Security System Policy.

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

Following the checks the Police, at their discretion, may advise an employer/ prospective employer that an individual is not acceptable 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 performance of companies installing remote signalling alarms will be monitored using Avon and Somerset Constabulary alarm statistics.

The formula published by the ACPO Security Systems Group will not be utilised.

ADMINISTRATION CHARGES **APPENDIX E**

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

1. Each application for a URN is subject to an administration fee payable by the system user. The URN Fee is £41.38 plus VAT and will be reviewed every two years by ACPO.

2. Upon receipt of the administration fee, a URN will be allocated to the system and issued to the maintaining company. If the applicant's cheque fails to clear, the URN will be cancelled and the security system company informed.

3. The administration fee is payable for:
   a) New URN applications
   b) New occupiers/owners of premises taking over existing security systems (system retains false alarm history unless upgraded to DD243 2004)
   c) Existing user changing security company (system retains false alarm history unless upgraded to DD243 2004)
   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 security company takes over another 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

5. In the event the installation does not proceed after the URN has been allocated, the fee is non-returnable

6. All security system monitoring centres operating under this policy must utilise the dedicated ex-directory lines nominated by each police force. An access fee may be chargeable and will be recovered by either a) the use of premium rate telephone call charges or b) an annual fee. The method chosen by the force is detailed at **Appendix A**.

7. If caller line identification is operated, central stations must not bar this facility on police calls.

8. 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.

APPENDIX F & G

These appendices are available as a separate download from the website in Word format.

APPENDIX H

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

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

NSI (National Security Inspectorate)
Sentinel House, 5 Reform Road, Maidenhead, Berkshire SL6 8BY
Tel: 01628 637512 Fax: 01628 773367 E-mail: nsi@nsi.org.uk
Website: www.nsi.org.uk

SSAIB (Security Systems & Alarm Inspection Board)
The Smoke Houses, North Shields, Tyne & Wear NE30 1JE.
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

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy. When documents are updated notification will be circulated throughout the organisation. Policy amendments may occur at any time and you should consult the principle electronic file if in doubt.

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.

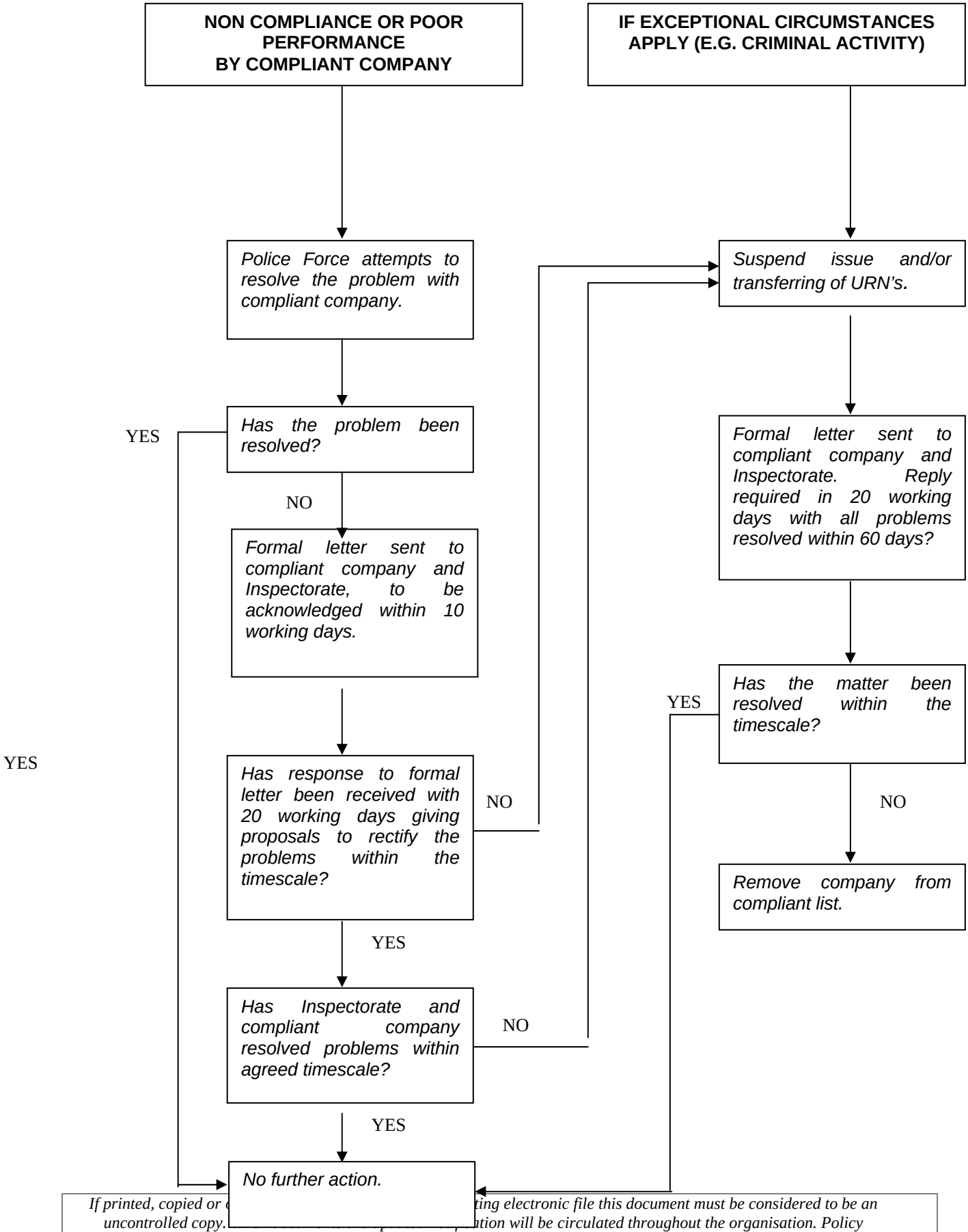
If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy. When documents are updated notification will be circulated throughout the organisation. Policy amendments may occur at any time and you should consult the principle electronic file if in doubt.

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.

APPENDIX J
MEMORANDUM OF UNDERSTANDING



APPENDIX K - Q

Appendices K – Q of the ACPO Policy will not be adopted by Avon and Somerset Constabulary.

APPENDIX R

REQUIREMENTS FOR COMPANIES INSTALLING AND MONITORING REMOTE CCTV SYSTEMS

1. INTRODUCTION

1.1 This document sets out the police requirements for remotely monitored detector activated CCTV systems to enable such systems to gain URNs from police forces.

1.2 Companies monitoring remotely monitored detector activated CCTV systems, known as RVRCs and Installers will ensure that these police requirements are brought to the attention of the users of such systems that require a police response.

1.3 Remotely monitored detector activated CCTV systems that are installed and monitored to the requirements stated in this policy, will be known as Type A systems and will be issued with a URN.

1.4 Systems for which police attendance may be required and which operate outside the procedures identified in the policy, will be known as Type B systems. URNs will not be issued to these systems.

1.5 The levels of police response to suspected crime reported by a Type A remotely monitored detector activated CCTV system, will be the same as that stated in the ACPO Security Systems Policy clause 3.1.

2. STANDARDS

2.1 Installers of remotely monitored detector activated CCTV systems will comply with all of the following standards and guidelines:

- ACPO Security Systems Policy
- BS 8418 Installation and remote monitoring of detector activated CCTV systems – Code of Practice
- BS EN 50132-7: CCTV Application guidelines

2.2 RVRCs monitoring detector activated CCTV systems will conform to all of the following standards:

- BS 5979 (Cat II):
- BS 8418: Installation and remote monitoring of detector activated CCTV systems – Code of Practice

3. LEGAL REQUIREMENTS

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

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy. When documents are updated notification will be circulated throughout the organisation. Policy amendments may occur at any time and you should consult the principle electronic file if in doubt.

4. PROCEDURES

4.1 The relevant police force will be sent a notice to install a remotely monitored detector activated CCTV system using Appendix F of the ACPO Security Systems Policy. A URN will be issued in line with the relevant police force policy (Appendix A of the ACPO Security Systems Policy refers).

4.2 The means of image collection and communication between the premises and the RVRC is a matter for the installer and the RVRC. However, the system will be installed to meet the requirements of Clause 2 of this appendix.

4.3 The system will be maintained in accordance with the BS 8418 Clause 13.1, and the requirements of the Data Protection Act 1998, CCTV Code of Practice (latest edition).

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy. When documents are updated notification will be circulated throughout the organisation. Policy amendments may occur at any time and you should consult the principle electronic file if in doubt.

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 of actual criminal activity in progress.

4.6 The RVRC operator will provide sufficient location and criminal activity information to the police control room.

4.7 The RVRC will employ filtering techniques to avoid unnecessary calls being passed to the police.

4.8 Any images required by a police force for investigative purposes will be supplied upon request.

4.9 The RVRC will send the recorded evidence (or at least a working copy) in the first instance to the investigating officer, with a completed statement of evidence to show continuity.

4.10 RVRCs using digital recording methods will adhere to the procedures for processing digital images, issued jointly by the Home Office, ACPO and PSDB.

5. MANAGEMENT INFORMATION

5.1 RVRCs will provide management information that is compatible to ACPO in relationship with the systems for analysis.

5.2 The information supplied will give a detailed analysis of the total number of calls passed to the police, registered with the URN.

5.3 Remotely monitored detector activated CCTV systems will be subject to the same conditions as laid down in the ACPO Security Systems Policy (Clause 3 refers) for the relevant police forces in relation to the total number of incidents incorrectly passed to the police.

5.4 The Memorandum of Understanding (MOU) is applicable to CCTV systems.

6. INDEMNITY

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

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy. When documents are updated notification will be circulated throughout the organisation. Policy amendments may occur at any time and you should consult the principle electronic file if in doubt.

APPENDIX S

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 Appendix A.

g. Ensure personnel who have access to third party security arrangements as a result of this process shall be subject to a security vetting procedure to British Standard 7858 or an equivalent, which identifies any unspent convictions or associations, which may be deemed unacceptable.

h. Be required to establish if certification has been given and/or withdrawn by any other Certification Body accredited to this scheme when an Installation, Maintenance or Monitoring Company makes application for acceptance.

i. Where disciplinary action is pending, in process or has resulted in expulsion by Certification Body 'A' of an Installation, Maintenance or Monitoring Company, for non-compliance with documents identified in

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy. When documents are updated notification will be circulated throughout the organisation. Policy amendments may occur at any time and you should consult the principle electronic file if in doubt.

Appendix A, the non-compliance causing the disciplinary action must be resolved prior to approval by another Certification Body 'B'.

j. Deal with any complaint against an Installation, Maintenance or Monitoring Company made by a police force in England, Wales & Northern Ireland, 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)

l. 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. Have financial stability to trade, at present and in the future.
Guidance - The certification body in determining financial stability to trade, may consider checking bank references, court orders and annual accounts prepared by an independent accountant, i.e. as provided to the Inland Revenue. In the case of an incorporated company the audited annual accounts or such accounts as are statutorily required should a company be exempt from audit.

c. Have adequate and relevant insurance in respect of employers, product, public, efficacy and wrongful advice liability.
Guidance - Insurance cover to a minimum of £1,000,000 per incident.

d. Have competent management with responsibility for all services provided.
Guidance – Management must be conversant with the relevant standards for the services they provide and be competent to inspect and test systems. Their responsibility extends to services provided by sub-contractors who must comply with all aspects of this document.

e. Have sufficient competent staff to carry out their contractual demands and the requirements of standards.
Guidance – The contractual demands and requirements of standards includes the design, planning, installation, system performance, operation, commissioning, false alarm management, complaint handling, maintenance and repair for security systems in accordance with the appropriate documents in Annexe A.

f. Have adequate arrangements, documented procedures and systems in place for all of their activities.
Guidance – This covers all aspects of a 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, 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.

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy. When documents are updated notification will be circulated throughout the organisation. Policy amendments may occur at any time and you should consult the principle electronic file if in doubt.

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. Have sufficient systems installed and/or monitored to enable competence and trading history to be determined.

j. 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 unfair business ethics.

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.

APPENDIX S (continued)

ANNEXE A

British Standards and European Norms (Latest Issue)

BS 4737	Intruder Alarms in Buildings
BS 7042	High Security
BS 7958	Closed Circuit Television Management – Management and Operation
BS 8418	CCTV Systems
BS 5979	Alarm Receiving Centres (Category II)
BS 6799	Wire free Alarms
BS 7858	Vetting of Security Personnel
PD 6662	Scheme for the application of European Standards for intruder and hold- up Alarm systems. (Attention is drawn to BSIA Form 171 - Guidance Notes)
BS EN 50131 series	Intruder & Hold up Alarms
BS EN 50132 series	Alarm systems – CCTV surveillance systems used in security applications – Application guidelines
BS EN 50136 series	Alarm Transmission systems
BS 7939	Smoke Security Devices
BS 8473	Management of False Alarms

British Standard Institute Drafts for Development (Latest Issue)

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

Vehicle Tracking

Category 5	Criteria for System Operating Centres December 2007
Category 5	Criteria for original Equipment Manufacturers September 2002

ACPO & Home Office Guidance	HOSB 14/02 Stolen Vehicle Tracking
CEN TS 15213 series	Road transport & traffic telematica- 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

APPENDIX T

TEN POINT PLAN FOR PERSONAL ATTACK DEVICES

1) FILTERING

The ARC's are not in a position to pass only confirmed PA's to the police. The fact that someone does not answer the telephone does not confirm the activation 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 intervention in place false calls will be reduced.

2) WITHDRAWAL OF POLICE RESPONSE

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

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

When a form of Intervention has been implemented, police response may be reinstated to PA's before the 3 month period. Any subsequent loss of response, after Intervention 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.

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

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy. When documents are updated notification will be circulated throughout the organisation. Policy amendments may occur at any time and you should consult the principle electronic file if in doubt.

facility is restricted to BS 7042 and EN 50131 grade 4 systems and not customer programmable. This will stop the duress signal being transmitted during watchdog failures or if the CIE reverts to default programming due to power problems.

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

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

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy. When documents are updated notification will be circulated throughout the organisation. Policy amendments may occur at any time and you should consult the principle electronic file if in doubt.

APPENDIX T (continued)

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.

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy. When documents are updated notification will be circulated throughout the organisation. Policy amendments may occur at any time and you should consult the principle electronic file if in doubt.

APPENDIX U

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 (AFSVIVR).

1.2 Only qualified and register personnel who meet these police requirements can installer AFSVIVR systems.

1.3 Systems operating centre (SOC) who meet these police requirements can monitor AFSVIVR systems.

1.4 A SOC must agree and sign the ACPO and Industry approved indemnity letter and return this to ACPO for distribution as part of the URN acceptance procedure.

1.5 A URN will be issued to a SOC for the purpose of monitoring AFSVIVR systems. This URN will be issued by ACPO.

1.6 The police response to a reported AFSVIVR system which meets the requirements set out in this appendix will be level .

1.7 Other types of vehicle tracking systems that operate outside of this policy will be know 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 REQUIRMENTS

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

2.2 INSTALLATION REQUIRMENTS

a. Installation shall be carried out by the car manufacturer at source or by a dealership or as an after market fit to the VFSVIVR manufacturers specifications.

b. The dealership or the after market fit shall only be undertaken by a company that is approved by an UKAS accredited inspectorate with ATSVIVR in their scope.

c. The AFSVIVR 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).*

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy. When documents are updated notification will be circulated throughout the organisation. Policy amendments may occur at any time and you should consult the principle electronic file if in doubt.

2.3 COMMISSIONING REQUIRMENTS

a. The commissioning of the AFSVIVR 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 a UKAS accredited inspectorate with AFSVIVR in their scope

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. HOSDB 14/02 – stolen vehicles
e. BS ISO 9001:2000
f. Inspected by a UKAS accredited inspectorate with AFSVIVR in their scope.

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 AFSVIVR 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.

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy. When documents are updated notification will be circulated throughout the organisation. Policy amendments may occur at any time and you should consult the principle electronic file if in doubt.

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.

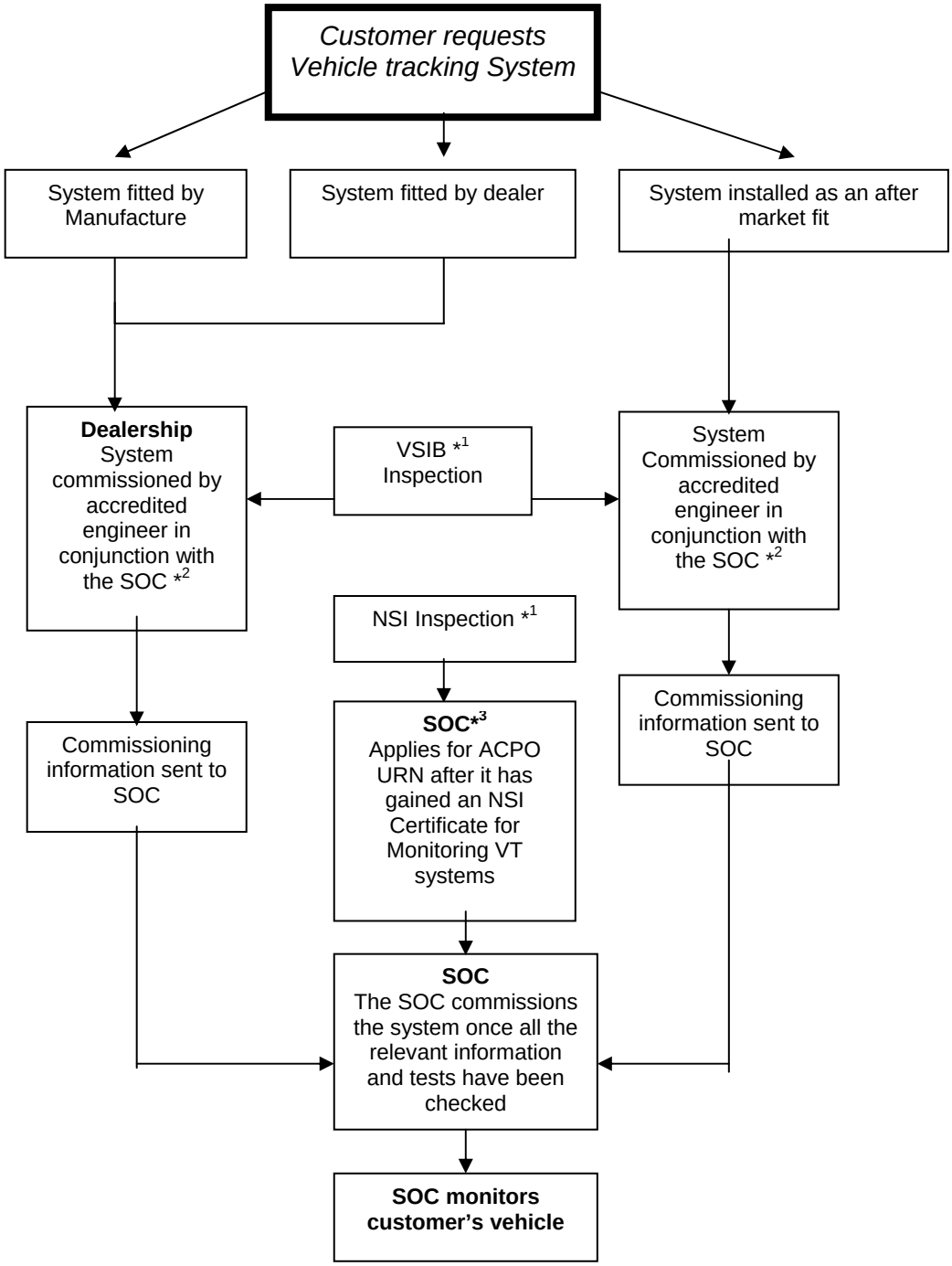
7. INDEMNITY

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 AFSVIVR system.

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy. When documents are updated notification will be circulated throughout the organisation. Policy amendments may occur at any time and you should consult the principle electronic file if in doubt.

Annexe A

ACPO VEHICLE TRACKING REQUIRMENTS FOR THE ALLOCATION OF A URN FOR A THATCHAM CATEGORY 5 STSTEM WITH VEHICLE IMMOBILISATION CAPABILITY



.

Notes:

*1 VSIB and NSI – UKAS accredited inspectorates.

*2 Accredited engineer shall be vetted (BS 7858 and have a police or CRB check).

*3 The SOC is to submit the approved indemnity letter to ACPO for circulation to Police forces.