

Police Service of Northern Ireland

HQ Ref: CSB/2006/2608/2

PD 01/06

POLICY DIRECTIVE

POLICE RESPONSE TO SECURITY SYSTEMS

1. POLICY IDENTIFICATION

POLICY TITLE: Police Response to Security Systems

POLICY OWNERSHIP:

DEPARTMENT	Criminal Justice
BRANCH	Community Safety

POLICY APPROVED BY:

CCF REF/OTHER	ACC Criminal Justice
DATE OF APPROVAL	5 September 2005

IMPLEMENTATION DATE: 9 February 2006

DATE OF ISSUE: 9 February 2006

DATE VERSION 3 ISSUED: 29 July 2008

REVIEW DATE: 30 July 2009

2. POLICY STATEMENT

(1) Policy

The Police Service of Northern Ireland (PSNI) will administer police response to alarm signals generated by electronic security systems to ensure that these are maintained to an agreed standard and the level of police response reflects the historical reliability of the alarm signal. In other words, systems, which are generating false alarms, will lose response if a defined threshold is reached.

(2) Glossary of terms

- (a) The term security '**company**' includes partnerships and sole traders.
- (b) **ARC** is the Alarm Receiving Centre, which receives alarm signals from monitored systems and passes details of activations to the Police.
- (c) **ACPO** is the Association of Chief Police Officers who provide guidance to all UK Police Services to ensure that the public obtain a broadly similar service from their local police, regardless of where they live.
- (d) **URN** is the Unique Reference Number of a monitored security system and is allocated by Alarms Administration Staff at Crime Prevention, Police HQ on application by a compliant security company. Where the policy refers to an alarm system or a security system this includes compliant CCTV and Vehicle Tracking Systems.
- (e) **Compliant Alarm Company** is a company which satisfies the conditions of this Policy and whose name appears on the list of compliant companies. Access to this list and all relevant forms can be gained by visiting www.psnipolice.uk/alarms or by contacting the Alarms Administration Unit at Police Headquarters.
- (f) **Type A** systems are those, which are monitored by a recognised ARC and are designed to send a signal to an ARC so that police may be informed, if required.
- (g) **Type B** systems are any systems, other than Type A (for example a bells-only alarm).
- (h) **UKAS** is the United Kingdom Accreditation Service, which is the sole national accreditation body recognised by government to assess, against internationally agreed standards, organisations that provide certification, testing, inspection and calibration services.
- (i) **NSI** is the National Security Inspectorate and **SSAIB** is the Security Systems and Alarms Inspection Board. Both are independent, not-for-profit approval bodies providing inspection services for the security and fire industries.
- (j) A **confirmed system** means a system, which is capable of confirming that an alarm activation is genuine, by one of three means. These are video, audio or sequential alarms.
- (k) A **false call** is an alarm call, which would normally be passed to police and has not resulted from:
 - (i) a criminal attack (or attempt) on the premises, the alarm equipment or the line carrying the alarm signal; **or**
 - (ii) actions by the Emergency Services in the execution of their duty; **or**
 - (iii) a call emanating from a personal attack system made with good intent.

Once an alarm activation has been passed to the police, it will be recorded as such on the Police Command and Control system and, if this transpires to be a false call, will count as a false activation as regards determining which response level applies to the premises. If police are contacted and informed that they need not attend (eg accidentally set off when locking up) the false activation will **NOT** be removed from the history log and will still count towards the maximum allowed in a rolling 12 month period.

(l) **A combination system** is a security system, which has a personal attack element and an intruder element. Where this type of system uses confirmed technology, false calls to each element are treated separately but the system has only one URN.

(m) **Senior Crime Prevention Officer** means the Inspector, Crime Prevention, Police HQ.

3. ADMINISTRATION

(1) Summary

(a) This Policy sets out how the PSNI will, in partnership with the Alarms Industry, set and maintain minimum standards for electronic intruder and personal attack alarms receiving police response and strive to reduce the number of false calls attended by police. A copy of the Policy can be downloaded from www.psni.police.uk/alarms.

(b) PSNI alarms Policy has been refined over a number of years to reflect changes in technology and service delivery. This has reduced the number of false calls, which police attend, but the ratio of false to genuine activations is still unacceptably high.

(2) Aims and Objectives

The Policy aims to:

(a) Reduce the waste of police resources by ensuring that police response is removed from systems which generate excessive false alarms.

(b) Reassure persons who purchase a monitored security system that:

(i) this can generate a reliable signal to an ARC to call for police response; and

(ii) the persons supplying, fitting and maintaining these systems satisfy the requirements of an Independent Inspectorate Body (NSI or SSAIB) and do not have unspent convictions for relevant criminal offences, especially those involving violence, dishonesty, sexual offences or drugs.

(c) Maintain a database of alarm users and keyholders to allow for monitoring and administration of the Policy.

(d) Maintain an up-to-date list of compliant alarm companies, which is available to the public either via the internet or from Crime Prevention, Police Headquarters.

(e) Inspect a sample of monitored security systems to ensure that these comply with the required standards.

(3) Legal Basis

(1) Police officers have a duty under Section 32(1) of the Police (NI) Act 2000:

(a) To protect life and property;

(b) To preserve order;

(c) To prevent the commission of offences;

(d) Where an offence has been committed to take measures to bring the offender to justice.

However, when the police receive information from an ARC of an alarm signal, it is only an indication that an offence **may** be taking place (currently more than 90% of alarm signals are false activations) and not evidence that an offence has been committed. There is no legal requirement for police to attend premises in response to every alarm activation. Decisions must often be made, based on a number of factors, including what other incidents police need to attend, the historical reliability of the security system and the availability of resources as to whether police attend immediately, when resources permit, or not at all.

(2) This Policy is based on the ACPO 'Police Response to Security Systems' Policy and complies with it. Both are 'living documents' and are, therefore, subject to change.

4. IMPLICATIONS OF THE POLICY

(1) **Financial and Efficiency Implications**

Reducing the number of false alarm calls attended by the police allows officers to provide a better response to other core policing issues. The implementation of this Policy ensures that waste of police resources is minimised, thereby reducing costs and increasing efficiency.

(2) **Human Resources/Training**

Police Control Room staff will receive guidance on aspects of the Policy which directly affect their role. Crime Prevention, HQ will facilitate as necessary.

(3) **Partnerships**

The ACPO Policy has been formulated in conjunction with the UK alarms industry and their Inspectorate Bodies.

(4) **Consultation**

Consultation on Police Response to Security Systems Policy takes place regularly with ACPO, the NI branch of NSI, BSIA and SSAIB.

5. HUMAN RIGHTS AND EQUALITY

(1) This Policy is deemed to be Human Rights compliant, has been screened for Section 75 considerations and meets the organisation's integrity standards.

(2) All parts of this Policy are suitable for public disclosure in accordance with the Freedom of Information Act 2000.

6. REVIEW

The Head of Community Safety Branch is responsible for reviewing the contents of this Policy on an annual basis.

7. PROCEDURE AND GUIDANCE

1. ANALYSIS

- (1) The number of false alarm calls attended by PSNI has reduced every year since major changes were made to ACPO/PSNI Alarms Policy in 2001.
- (2) PSNI Alarms Administration Unit will continue to closely monitor alarm calls to ensure that this Policy is being adhered to.

2. PREVENTION AND REASSURANCE

Effective use of a security system not only detects criminals on the premises but also acts as a deterrent to a variety of crimes.

3. PATROL

Reducing attendance at false calls increases the confidence for response officers that an activation is due to criminal activity. This, in turn, increases the likelihood of detaining intruders on the premises.

4. APPLICATION OF THE POLICY

- (1) To enable a security system to qualify for police response, it must comply with this Policy and a recognised standard or code of practice controlling manufacture, installation, maintenance and operation. Such standards must be in the public domain and must not be product based.
- (2) Compliant Companies must be inspected and recognised by an UKAS Accredited Inspectorate Body acceptable to ACPO/PSNI, which demonstrates to the Senior Crime Prevention Officer that Northern Ireland logistics and/or viability factors will not detract from the quality and quantity of supervisory inspections.
- (3) Where a security company loses police recognition (ie is removed from the list of compliant companies), customers will be required to make alternative arrangements with another Compliant Company within **three months**. Where an ARC loses police recognition, customers will be required to make alternative arrangements with another compliant ARC within **six months**. Failure to make alternative arrangements will result in the deletion of the URN. The issue of a new URN enabling the restoration of police response will only occur when Alarms Administration are satisfied that the system now complies with current standards, and would then incur an administrative charge.
- (4) Logistics dictate that Compliant Companies must have an address in Northern Ireland and have engineers based here with a 4-hour maximum response time.

5. SCOPE OF THE POLICY

(1) Type A - Remote Signalling Systems

These are systems terminating at a recognised Alarm Receiving Centre (ARC), Remote Video Response Centre (RVRC) for CCTV or System Operating Centre (SOC) for vehicle tracking. All centres must conform to BS 5979 (Cat II).

- (2) In the case of vehicle tracking systems, one URN will be issued to the monitoring centre, not to each vehicle.
- (3) ARCs dealing solely with alarm systems within their own company premises (in-house monitoring), are exempt from the BS 5979 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, ie no 3rd party commercial risk is undertaken; and
- (c) the intruder alarm systems are operated in accordance with all other aspects of this Policy.

(3) **Type B - Security Systems**

URNs will not be issued to security systems, which operate outside procedures identified at paragraph 7(5)(1) above.

6. POLICE RESPONSE TO AN ALARM ACTIVATION

- (1) For Type A security systems there are **two** levels of police response:

(a) **LEVEL 1 – Immediate/Urgent response**

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

(b) **LEVEL 3 – Response Withdrawn**

No police attendance, keyholder response only.

- (2) The PSNI has adopted a policy on the use of confirmed alarm technology as part of the effort to reduce false calls. All new applications will only qualify for a URN and police response if alarm activations are to be 'confirmed' before being passed to the police. Where a URN has been deleted for any reason, a new application will be required if police response is desired.
- (3) Activation of detectors (without apparent damage or entry to the premises) and line faults will be treated as false alarms unless proved otherwise.
- (4) Alarm activations initially recorded as false, which transpire to be genuine, can only be treated as such if the PSNI, Alarms Administration Unit is notified (with accompanying evidence) within 14 days.
- (5) New security systems (or applications for a URN where a previous URN has been deleted for any reason) must comply with the latest standard. This is currently PD6662 Grade 2 or above. Security systems issued with a URN will initially receive Level 1 response.
- (6) Following the first false call in a rolling 12 month period the customer will be advised in writing, by the Alarms Administration Unit, with a copy being forwarded to the maintaining alarm company. Following **two** false calls to personal attack activations or **three** false calls to intruder activations in 12 months LEVEL 3 will apply and police response will be withdrawn. The customer will be advised in writing with a copy to the maintaining company, who will be required to instruct the ARC/RVRC not to pass alarm messages to the police. For confirmed combination systems the withdrawal will only apply to the part of the system, which has reached the appropriate threshold. For an unconfirmed combination system, withdrawal of response to one part will result in withdrawal of response to the whole system and deletion of the URN.
- (7) Following withdrawal of response, the following conditions will apply in order that police response can be restored:
- (a) Unconfirmed systems will need to be upgraded to Confirmed DD243 (2004) systems;
 - (b) Confirmed systems which are not DD243 (2004) will have to be upgraded to DD243 (2004) systems;

- (c) Confirmed DD243 (2004) systems will have to wait until they have been free of false calls for 3 months (supported by evidence from the alarm company) or have a second form of confirmation installed;
 - (d) PD6662 (2004) systems will have to wait until they have been free of false calls for 3 months (supported by evidence from the alarm company) or have a second form of confirmation installed.
- (8) Where a system has been upgraded, the police will require a certificate of installation. In all cases above, if restoration of response is desired, application for restoration must be made not more than 6 months after the date when response was withdrawn. If a system is off response for more than 6 months (either due to continuing false calls or a failure to submit the appropriate application), the URN will be deleted and any subsequent application will be treated as an application for a new system.
- (9) PSNI 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.

7. CCTV SYSTEMS

To enable remote detector activated CCTV systems to gain a URN for police response, they must comply with:

- (1) PSNI Electronic Security Systems Policy;
- (2) BS 8418 (Code of Practice); and
- (3) EN 50132-7 (CCTV application guidelines).

8. PERSONAL ATTACK ALARMS (PA)

- (1) A deliberately operated device (PA) may be operated to summon urgent police assistance when an assailant enters a previously defined area with the obvious intention of harming or threatening any person within that area. If the device is portable it will not require any additional information concerning its location, other than the address of the premises. These devices must not be used to summon assistance in circumstances other than this (eg a motorist driving off without paying for fuel). Misuse to summon police attendance to non-attack incidents will be treated as a breach of this Policy and may result in withdrawal of response.
- (2) In a system with both PA and intruder facilities the remote signal must differentiate between the two types. Unless this distinction is made, any withdrawal of police response sanction will apply to all calls from the system.
- (3) Response may be reinstated to PAs before 3 months free from false calls, if the alarm company can satisfy the Senior Crime Prevention Officer that a significant change has been made to that particular system to prevent further false calls. Re-instatement in this way can only be obtained once.

9. TYPE B (UNMONITORED) SECURITY SYSTEMS

- (1) To obtain police response, Type B systems will require some additional indication from the scene that a criminal offence requiring police attendance is in progress. This will be as a result of human intervention such as member of public, owner or agent visiting or viewing the premises and the level of police response will depend on the quality of the information received. The addition of electronic means to provide confirmation will not promote such systems to Type A or achieve police response. Calls for police attendance should be by telephoning 999 or via the non-emergency numbers, 0845 600 8000, as appropriate.
- (2) Automatic dialling equipment **must not** be programmed to call police telephone numbers.

- (3) Calls received from non-compliant ARCs/RVRCs and calls from compliant ARCs/RVRCs without a valid URN **will not** receive a police response.

10. COMPLIANT SECURITY COMPANIES INSTALLING TYPE A SYSTEMS

- (1) To identify companies conforming to this Policy the PSNI hold a list of compliant companies. Inclusion on the list does not mean that the police have inspected the company, or its work. Only companies so listed may install, maintain and/or monitor Type A systems in Northern Ireland. 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) Companies applying for inclusion on the above list must do so using form **Appendix 'B'** and must:
 - (a) be inspected and recognised by an independent inspectorate body as at paragraph 7(4)(2); and
 - (b) not have as a principal or employee in the surveying, sale, installation, monitoring, maintenance or administration of security systems, persons with relevant criminal convictions (other than spent convictions). Relevant convictions include but are not limited to those involving violence, dishonesty, sexual offences or drugs. Form **Appendix 'C'** sets out the procedure for the implementation of this requirement and all decisions, by Crime Prevention, on whether a person is suitable or unsuitable will be documented and audited.
- (3) Whilst convictions will only prevent a person from being deemed suitable if they are 'relevant', **every** unspent conviction (including motoring offences) must be declared, by applicants as the decision as to what convictions are 'relevant' rests with the Senior Crime Prevention Officer.
- (4) Applicants for employment with compliant security companies **must not be appointed** to posts involving the sales, surveying, installation, monitoring or administration of security systems until written notification is received from Crime Prevention that they are suitable.

11. APPLICATION FOR A URN FOR A TYPE A SECURITY SYSTEM

- (1) Prior to the signing of a contract the installing company must give the customer a document outlining the police Policy. (Form **Appendix 'I'**).
- (2) Notice of intention to install a Type A security system requiring a URN, must be sent to the Senior Crime Prevention Officer on form **Appendix 'F'**.
- (3) When the Police Alarms Administration Unit issue a URN, this 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 will not receive a police response without additional evidence of an offence in progress.
- (4) Only 1 URN will be issued for each system, regardless of whether this is Intruder Only, Personal Attack Only or a Combination System.
- (5) The form **Appendix 'F'** must contain the grid reference for the premises in which the system is to be installed. This must either comprise 12 digits or 2 letters and 10 digits and must be taken from the **Irish Grid**. Applications submitted without a valid grid reference will be returned unprocessed.

12. INSPECTIONS

The PSNI inspect security systems to test their compliance with the Policy. Refusal to allow an inspection of a system will result in removal of police response and the URN will be deleted. Alarm companies must facilitate these inspections to remain on the list of compliant companies.

13. ABANDONED INSPECTIONS

- (1) A scheduled inspection of a system will be deemed to be abandoned if:
 - (a) Either a representative from the premises or an alarm engineer familiar with the system fails to attend; or
 - (b) It is cancelled at short notice (48 hours or less); or
 - (c) On re-inspection, **all** remedial work has not been completed.
- (2) If an inspection is abandoned, the URN may be deleted.
- (3) Where an excessive amount of inspections are abandoned this will be treated as a breach of Policy and the company will be refused any chargeable events for a period of 28 consecutive days.

14. SYSTEMS WHICH FAIL AT INSPECTION

- (1) Failure is designated as either Fail 'A' or Fail 'B'; full details of the requirements are at www.psnipolice.uk/alarms. Fail 'A' will require the system to be re-inspected after rectification whereas Fail 'B' will not normally require re-inspection if the faults found are rectified by the engineer and a certificate to that effect submitted, by the alarm company, to the Alarms Administration Unit within 2 months.
- (2) Where a system fails at re-inspection the URN will be deleted and a new application required if police response is sought.

15. ENGINEER TESTS/LEVEL 3 SIGNALS FORWARDED TO POLICE CONTROLLERS

- (1) An Engineer test forwarded to a Police Controller will be treated as a false call from the system that generated the signal. Where an excessive number of engineer tests from the same alarm company are passed to police, that company may be treated as being in breach of this Policy.
- (2) Where a system on Level 3 response (keyholder only) generates a signal, which is forwarded to the police, this will be treated a breach of this Policy. On the first occasion, the security company will receive a written warning. On the 3rd occasion in any rolling 12 month period, the security company will be refused any chargeable events until no Level 3 activations have been forwarded for at least 28 consecutive days.

16. VARIATIONS

Any variations to the original URN application details must be notified within 28 days to the Senior Crime Prevention Officer on form **Appendix 'G'**. Failure to do so will result in the URN being deleted and a new application would then be required. **Appendix 'G'** can be downloaded from www.psnipolice.uk/alarms or obtained by contacting the Alarms Administration Unit at Police Headquarters.

17. KEYHOLDERS

- (1) All premises with Type A systems must have at least two keyholders, details of whom will be maintained by the Police Alarms Administration Unit. A change to keyholder details is a variation to the application and must be forwarded to the Senior Crime Prevention Officer on form **Appendix 'G'** within 28 days.
- (2) Keyholders must be trained to operate the alarm, be telephone subscribers, have suitable means of transport to attend the premises at all hours, have access to all relevant parts of the premises and be able to attend within 20 minutes of being notified. Keyholders must not reside at the same address as the alarmed premises.
- (3) Customers who employ a commercial keyholding company must be aware of the Security Industry Authority Licensing Regulations in relation to keyholding and response.

- (4) Failure of keyholders to attend when requested will, on the first occasion, result in a written warning. Failure to attend on 2 occasions in a rolling 12 month period or refusal to attend on any occasion will result in the withdrawal of police response for a period of 3 months. The procedure for restoration will be as at paragraph 7(6)(7) above. Where no keyholder can be contacted, this will be treated as failure of keyholder.
- (5) If a keyholder wishes to appeal an event recorded as a failure to attend within the specified 20 minutes, this can only be considered if accompanied by written evidence from the ARC (eg printout of Event Log).

18. DELAYS OF AUDIBLE SOUNDER AND ALARM ACTIVATED SECURITY DEVICES

No time delay is required and instantaneous sounders are acceptable.

19. ADMINISTRATIVE CHARGES

- (1) Where a **chargeable event** occurs, this is subject to an administration fee payable to the Police Service of Northern Ireland. The fee is currently £45 inclusive of VAT.
- (2) The following are **chargeable events**:
 - (a) Application for a URN for a new system;
 - (b) Change of alarm company for a system currently on police response;
 - (c) Change of client for a system currently on police response;
 - (d) Change of trading name for a system currently on police response;
 - (e) Application for a new URN for an existing system because the previous URN has been deleted (for any reason).
 - (f) Where an unconfirmed system is upgraded to confirmed technology whilst still eligible for Level 1, a new URN will be issued but **the fee will be waived**.

Where several of the above events occur at the same time only 1 fee will be charged.

Where a security company takes over another security company – no charge is made and the systems retain their alarm history.

- (3) URNs will only be issued to compliant alarm companies registered with the PSNI and only on submission of form **Appendix 'F'**.
- (4) Companies are required to purchase 'credits' in advance of allocation of URNs to their customers. The URN 'credits' will be available in blocks to suit the scale of the Company's activities. URNs will only be released where the requesting Company is in credit with the Alarms Administration Unit. The Senior Crime Prevention Officer will determine block size for each company and the threshold at which an invoice for another block of URNs is raised.
- (5) Once an invoice for a block of URNs is issued, payment must be made within 30 days. Failure to pay within this period will result in the company being refused further URNs until 28 days after funds are received. Persistent late payment of invoices will be treated as a breach of this Policy and may result in the company being refused URNs for a longer period, being reported to their Inspectorate Body and/or being removed from the list of compliant companies.
- (6) All communications between Alarm Companies and the PSNI Alarms Administration Unit will be on the prescribed forms. These will be available:
 - (a) in hard copy paper originals for photocopying from the Alarms Administration Unit;
 - (b) To download, in 'Word' format, from the PSNI website. (www.psnipolice.uk/alarms)

20. TRANSFER OF ALARM SYSTEMS

(1) **Between Companies - Chargeable**

Where a system is transferred between companies the new company must apply to the Alarms Administration Unit for the transfer of the URN. This must be supported by a copy of the written confirmation, from the customer to the previous Company, terminating the existing contract.

(2) The Alarms Administration Unit will not become involved in disputes between existing/new companies and customers.

(3) Cancellations notified to the Alarms Administration Unit on form **Appendix 'G'** will be held for 28 days to facilitate takeovers and to avoid deletion of the URN.

(4) **Between Clients – Chargeable**

Where an existing system has a change of client this must be notified on form **Appendix 'G'** within 28 days. The false alarm history of the system will be retained unless the system is upgraded to current standards.

(5) **Change of Trading Name - Chargeable**

Where an existing system has a change of trading name this must be notified on form **Appendix 'G'** within 28 days.

(6) Failure to notify Alarms Administration Unit of changes to details within the time limit may result in the URN being deleted.

(7) **Transfer of URN**

The URN remains, at all times, the property of the PSNI and can only be transferred by application to the Alarms Administration Unit. Any attempt to circumvent this procedure will be treated as a breach of policy.

21. MEMORANDUM OF UNDERSTANDING

For non-compliance or poor performance by a Compliant Security Company or ARC/RVRC, the procedure set out in the Memorandum of Understanding may be considered before suspension of URNs. (Form **Appendix 'J'**).

22. ADVERTISING

Installation companies, ARCs and Inspectorate Bodies must not use terminology which might raise in the mind of the customer an unrealistic expectation of police response to a security system and will not use the PSNI Crest or ACPO Logo in advertising material. Wording such as 'Police Approved', 'Police Preferred', 'Police Compliant', 'Meets Police Requirements' or similar must not be used.

23. LIABILITY AND FINAL DISCRETION

(1) This Policy does not impose any liability on the PSNI, its officers or employees nor the Northern Ireland Policing Board (NIPB) arising out of any acts or omissions connected with security systems. This includes failure to respond or timeliness in responding to any activation. Policing requires that resources are tasked to attend the most urgent calls first and no duty to provide a specific level of response is implied by this Policy or guaranteed by compliance with it.

(2) The Senior Crime Prevention Officer, acting on behalf of the Chief Constable, 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) alter, amend or add to this Policy through the ACPO Security Systems Group.