



IPCRes **guidance**

InFiReS
Insurers' Fire Research Strategy funding scheme

The selection and use of electronic security systems in empty buildings



Fire Protection Association

Protecting people, property, business and the environment

London Road
Moreton in Marsh
Gloucestershire GL56 0RH

Insurers' Property Crime Research (IPCRes) working group

This guidance document has been developed by the IPCRes working group of InFiReS (see below). IPCRes publications continue the tradition of providing authoritative guidance on crime prevention topics which was established by the Crime Panel of the Association of British Insurers.

Important notice

This document has been developed through the Insurers' Fire Research Strategy scheme (InFiReS) and published by the Fire Protection Association (FPA). InFiReS membership comprises a group of UK insurers that actively support a number of expert working groups developing and promulgating best practice for the protection of people, property, business and the environment from loss due to fire and other risks. The technical expertise for this document has been provided by the Technical Directorate of the FPA, external consultants, and experts from the insurance industry who together form the various InFiReS Steering Groups. Although produced with insurer input it does not (and is not intended to) represent a pan-insurer perspective. Individual insurance companies will have their own requirements which may be different from or not reflected in the content of this document.

The FPA have made extensive efforts to check the accuracy of the information and advice contained in this document and it is believed to be accurate at the time of printing. However, the FPA make no guarantee, representation or warranty (express or implied) as to the accuracy or completeness of any information or advice contained in this document. All advice and recommendations are presented in good faith on the basis of information, knowledge and technology as at the date of publication of this document.

Without prejudice to the generality of the foregoing, the FPA make no guarantee, representation or warranty (express or implied) that this document considers all systems, equipment and procedures or state-of-the-art technologies current at the date of this document.

Use of, or reliance upon, this document or any part of its content is voluntary and is at the user's own risk. Anyone considering using or implementing any recommendation or advice within this document should rely on his or her own personal judgement or, as appropriate, seek the advice of a competent professional and rely on that professional's advice. Nothing in this document replaces or excludes (nor is intended to replace or exclude) entirely or in part mandatory and/or legal requirements howsoever arising (including, without prejudice to the generality of the foregoing, any such requirements for maintaining health and safety in the workplace).

Except to the extent that it is unlawful to exclude any liability, the FPA accepts no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from the publication of this document or any part of it or any use of or reliance placed on the content of this document or any part of it.

First published by

The Fire Protection Association

London Road

Moreton in Marsh

Gloucestershire GL56 0RH

Tel: +44 (0)1608 812 500 Fax: +44 (0)1608 812 501

E-mail: sales@thefpa.co.uk Website: www.thefpa.co.uk

2007 © The Fire Protection Association for InFiReS ISBN 1-902790 54-5

Copies of this document may be obtained from the publications department of the FPA, at the above address, or by calling +44 (0)1608 812 500 or e-mailing sales@thefpa.co.uk.

Printed in Great Britain by Modern Colour Solutions. 2.0/11.07

Contents

1.	Introduction	4
2.	Why use electronic security systems?	4
3.	Intruder alarm systems	4
	3.1 Conventional intruder alarm systems	4
	3.2 Temporary intruder alarm systems	5
4.	Closed circuit television (CCTV)	6
	4.1 Conventional CCTV systems	6
	4.2 Temporary CCTV systems	6
5.	Conclusion	7
	Appendix: Temporary security systems: Owners' checklist	8

1. Introduction

This document provides guidance on the subject of electronic security systems for empty buildings to assist those considering installing such systems. It supplements the Insurers' Property Crime Research (IPCRes) group publication, *The protection of empty buildings*, which provides comprehensive information regarding the problems often associated with empty buildings, together with guidance concerning possible safeguards. In order to set the scene for what follows, this current document briefly restates some of the principles outlined at greater length in *The protection of empty buildings*.

The appendix to this document outlines ideal specifications for temporary security systems.

By way of clarification, and to avoid unnecessary repetition/qualification within the body of this document, the following terms are considered to mean:

- *owners* – those responsible for the empty building. According to the circumstances of the building, this could be those who own the building, leaseholders, tenants, or managing agents and their staff;
- *building(s)* – land and any structure/property built upon it, plus any contents within;
- *empty building(s)* – buildings that, to all intents and purposes, are not being used as a workplace, store or as accommodation.

2. Why use electronic security systems?

Empty buildings are prone to various common problems, such as deterioration of the fabric, damp, escape of water, fly-tipping, fly-posting and external vandalism etc. Many of these problems can be eliminated or reduced by good management, including regular inspections and appropriate maintenance and repair. However, empty buildings are often additionally at risk of being accessed by trespassers or intruders for various activities, such as squatting, illegal trading (including drugs), parties (raves), internal vandalism and theft of contents or fixtures and fittings. There may also be a significant risk of partial or complete destruction by fire, particularly as a result of arson.

Physical security is often put in place to deter or hinder unauthorised access, but this may not be practical or sufficient in every case to prevent intruders gaining access. Therefore, some means of alerting the owners to unauthorised access will often be necessary to fully manage the risks mentioned above. This usually involves the use of an intruder alarm system, although sometimes a remotely monitored CCTV system may also prove suitable.

3. Intruder alarm systems

Intruder alarm systems can be considered under two headings, namely 'conventional' and 'temporary' alarm systems.

3.1 Conventional intruder alarm systems

Many buildings in normal use are fitted with a permanently installed, mains-powered, internal intruder alarm system. To install such an alarm system in a building once it is empty can involve considerable expense and delay. Therefore, wherever possible, as a building becomes vacant, any existing alarm system should be retained or formally taken over by the new owner and then maintained/upgraded as appropriate to provide ongoing intruder detection.

Conventional alarm systems are usually installed, maintained and monitored by installing companies and alarm receiving centres (ARCs) that have been third-party accredited by an inspectorate body such as the National Security Inspectorate (NSI) or the Security Systems and Alarms Inspection Board (SSAIB). This accreditation is supported by insurers and other interested bodies, including the police, as a means of ensuring that relevant British (BS) and European (EN) standards are complied with for alarm system design, maintenance, ARC monitoring, security procedures, record-keeping and staff security vetting.

According to current police security system policy (SSP) rules, NSI/SSAIB accreditation of the installation company, maintenance company or monitoring company is a prerequisite for obtaining a routine emergency police response to alarm activations. Owners of systems meeting all the requirements of the police SSP rules can apply for a police unique reference number (URN), and thus be automatically eligible for a routine emergency police response to qualifying activations.

Regardless of whether a system qualifies for police response, it is essential to ensure that appropriate arrangements are made to respond to any alarm faults/activations by the appointment of suitable in-house or commercial premises keyholders. For further guidance on the appointment of keyholders, please refer to the IPCRes document *Electronic security systems: Guidance on keyholder selection and duties*.

3.2 Temporary intruder alarm systems

Where an empty building has no alarm system, or it proves impractical to take over and use an existing system – for example, if previous owners have removed or damaged components, or the necessary mains power supply is no longer available – it is often possible to install a temporary alarm unit or system.

Temporary alarm systems usually comprise a portable control/power unit and various wire-free intruder alarm sensors, although some use various forms of audio or visual detection and/or verification. Fire detection sensors can be added to some systems. Temporary alarms are designed to be powered by a battery, although mains power can sometimes be utilised, if present on site. Low battery power indications are usually sent to the ARC.

Most systems provide silent or covert notification of activations to an ARC via the mobile phone (global system for mobile communications (GSM)) network, but some have an option to use additional on-site sirens/sounders. Some products can also send periodic test calls to and from the site to check the operational status of the system and the means of notification.

Various specialist companies can provide temporary alarm products/services. Due to the niche nature of this activity, the majority of such companies do not seek NSI/SSAIB accreditation, partly because there are few relevant BS/EN standards that specifically apply to such systems. Nonetheless, some form of external accreditation of all or some of the provider's activities is desirable, and owners may wish to select a provider on the basis of this criterion.

As temporary intruder alarm systems do not meet applicable police rules (see section 3.1), they do not qualify for a URN and a routine emergency police response. Some system providers undertake to ring the local police via normal telephone lines to alert them to verified alarm activations, but this practice is generally discouraged by senior police officers and therefore users should make no assumption that this will happen. It is therefore essential that owners put in place adequate and reliable arrangements for private or commercial keyholders to attend the alarm-protected site to investigate or rectify the cause of any alarm activation or fault.

If arrangements are made for owners' in-house keyholders to attend activations, they should be cautioned to do so with due regard for their safety, and advised to:

- attend in pairs;
- let someone know where they are going and when they can be expected to make contact/return;
- carry mobile phones;
- be aware that if there are signs of a break-in, or suspicion that intruders are present, they should call for police assistance via the 999 telephone network.

Many commercial companies provide a response and keyholding service and building owners often choose to employ such services to avoid some of the difficulties that can arise with the use of in-house keyholders. Again, the IPCRes publication, *Electronic security systems: Guidance on keyholder selection and duties*, provides further

information and advice. Owners should ensure that any company employed to provide such a service meets with the full approval of their insurers.

The ideal specification of a temporary intruder alarm system is outlined in the Appendix to this document. While temporary alarms are a cost-effective and proven way of providing protection against intrusion into empty buildings, their effectiveness will depend on many factors. Owners should therefore satisfy themselves as to the suitability and effectiveness of any system under consideration by comparing the system to the 'ideal' specification given in the Appendix.

4. Closed circuit television (CCTV)

CCTV takes many forms, but to be effective, a system needs to be monitored so that unauthorised persons approaching or entering the building may be challenged and/or a keyholder or response service dispatched to attend.

CCTV systems can be considered under two headings, namely 'conventional' and 'temporary'.

4.1 Conventional CCTV systems

The cost of installing a new, conventional, monitored CCTV system to protect an empty building, particularly for a short period, will usually be prohibitive. However, in some cases it may be possible to take over a system which has already been installed in the building, or to arrange for a system covering an adjacent site/public space, such as a town or shopping centre system, to monitor the empty building.

The complexity of conventional CCTV systems is such that they should only be assumed to be effective where installed, maintained and monitored by companies that have been third-party accredited by an inspectorate body such as the NSI or the SSAIB. As with intruder alarms, this accreditation is supported by insurers and other interested bodies, including the police, as a means of ensuring that relevant British/European standards are complied with for system design, maintenance, monitoring, security procedures, record-keeping and staff security vetting. Existing systems without such accreditation should be evaluated by a reputable consultant to establish if cost effective action is feasible and desirable to optimise their potential.

According to current police rules (see section 3.1), NSI/SSAIB accreditation is a prerequisite for obtaining a routine police response to alarm activations generated by CCTV systems connected to a monitoring centre. To qualify for an emergency police response via a monitoring centre. CCTV system must meet police rules and be granted a URN.

4.2 Temporary CCTV systems

If arrangements cannot be made for a suitable existing system to monitor the empty building, a temporary CCTV system may be the only cost-effective solution if visual evidence of activities at an empty building is required. Devices are currently available which consist of an enclosure housing a battery power supply, passive infra-red movement detector (PIR), camera with infra-red illumination, GSM unit and a key switch.

A few specialist companies can provide temporary CCTV products/services. Due to the niche nature of this activity, the majority of such companies do not seek NSI/SSAIB accreditation, partly because there are few relevant BS/EN standards that specifically apply to such systems. Nonetheless, some form of external accreditation of all or some of the provider's activities is desirable, and owners may wish to select providers on the basis of this criterion.

As temporary CCTV systems do not meet police rules (see section 3.1), they do not qualify for a URN and a routine emergency police response. However, some providers undertake to ring the local police via normal telephone lines to alert them to visually verified system activations. The chances of this resulting in a police response are increased if the monitoring operation can persuade the police operator that a criminal act has taken place or is likely to take place. Note, however, that trespass, in itself, is a civil, rather than criminal, offence.

As with temporary intruder alarms, it is essential that owners put in place adequate and reliable arrangements for private or commercial keyholders to attend the CCTV-protected site to investigate or rectify the cause of any system activation or fault.

5. Conclusion

Wherever practical, it will usually be preferable to utilise or adapt an existing conventional electronic security system for the monitoring of an empty building. However, where this cannot be achieved, temporary electronic security systems can be an effective means of monitoring, particularly when coupled with appropriate physical security measures and suitable deterrent warning signs on site.

The main advantages of installing a temporary electronic security system compared with a conventional system are:

- speed of installation;
- no requirement for mains power;
- no requirement for a telephone line;
- reduced costs – temporary systems are usually hired by the week/month;
- ease of relocating units/detectors as a result of wire-free technology;
- commercial providers can provide services such as response to system activations, regular site inspections, waste clearance and boarding-up services etc.

There are a number of companies that specialise in the provision of site surveys, installation, maintenance, monitoring and response to temporary electronic security systems in vacant buildings. While most of these companies do not meet all of the traditional standards/inspectorate 'benchmarks' familiar in the field of conventional electronic security systems, most are dealing with the specific issues relating to the protection of vacant property on a daily basis. They are therefore likely to have the expertise and resources available to adequately deal with most problems encountered.

Appendix

Temporary security systems: Owners' checklist

When choosing a temporary security system, owners should consider the following issues. They should also seek advice/approval from any interested insurer.

Building/design issues

- Does the system under consideration provide the required level of alarm/CCTV protection?
- Are the areas requiring protection suited to the proposed detection, ie free from undue vibration, vermin and birds etc that are likely to cause false alarms?
- Does the system provide the required number of control units/detection devices necessary to protect the building?
- Can control unit(s) be sited within an alarm-protected and/or a secure area?

System providers/installers

- Does the system provider carry out installation rather than subcontracting installation to another company?
- Do the installers hold any third-party inspectorate accreditation or otherwise operate to relevant standards, such as BS 7858: 2006: *Security screening of individuals employed in a security environment. Code of practice* or BS EN ISO 9001: 2000: *Quality management systems*?

System equipment

- Can the control unit be physically fixed in place?
- Is the control unit strong enough to be likely to resist physical attack while sending any system activation message to the ARC?
- Is the expected battery life of the control unit at least 3 months?
- Will detection devices send low battery power signals to the control unit?
- Will the control unit send low battery power signals to the ARC?
- Will a record of alarm setting/unsetting and activations be captured at the ARC or in the site control unit?
- What maintenance checks are advised?

Alarm notification (signalling)

- Will a reputable company be acting as the monitoring centre for the system?
- Does the monitoring centre operate 24 hours a day, 365 days a year?
- Does the monitoring centre hold any third-party inspectorate accreditation or otherwise operate to a relevant standard, for example BS 5979: 2000: *Code of practice for remote centres receiving signals from security systems*?
- Can test calls be sent between the control unit and the monitoring centre, and will these be sent with sufficient frequency?

Response

- Can suitable arrangements be made for premises keyholders to be notified of and respond to any activations/faults?
- If a commercial response and keyholding company will be used, does the company hold third-party inspectorate accreditation or otherwise operate to a relevant standard, such as BS 7858: 2006: *Security screening of individuals employed in a security environment. Code of practice*; BS 7984: 2001: *Keyholding and response services. Code of practice*; or BS 7499: 2002: *Static site guarding and mobile patrol services. Code of practice*?
- If a commercial response/guarding service will be employed, is the providing company listed as an approved contractor by the Security Industry Authority (SIA)?
- Are any response times for the commercial response and keyholding service guaranteed?