Dated: **10 January 2007**

To: **All NSI NACOSS Gold and NSI Systems Silver Approved Companies, all applicants for NACOSS Gold and Systems Silver Approval, all NSI ARC Gold Approved Companies and all Applicants for ARC Gold approval**

TECHNICAL BULLETIN No. 0004

Guidance on the implementation of BS 8473:2006, the British Standard Code of Practice for Intruder and hold-up alarm systems – Management of false alarms (Supersedes BSI DD 245:2002)

The new British Standard Code of Practice, BS 8473:2006 (Incorporating Corrigendum No.1), supersedes British Standards Institution (BSI) Draft for Development DD 245:2002, which previously superseded NSI Code of Practice NACP 10 (Issue 2). The Foreword to BS 8473 references 1st March 2007 as the date the new Standard is intended to come into effect. The Standard is now available through licensed outlets including NSI who can supply copies at a discounted rate.

BS 8473:2006 will now be applied to all organisations that wish to obtain or maintain NSI Approval for any scheme that requires compliance with this Standard. Even though BS 8473:2006 shows an effective date of 1st March 2007, organisations may elect to apply the Standard with immediate effect, subject to the additional clarifications and guidance within this Technical Bulletin and subject also to agreement between the parties involved.

With immediate effect, applicant organisations will be assessed against BS 8473:2006 and any non-compliance recorded against clauses of the Standard will have to be satisfactorily addressed before approval can be granted.

Existing NSI Approved Companies will however be given until 30th June 2007 to fully comply with the revised requirements. In the interim, Non-Compliance Reports will be issued for any of the revised requirements within BS 8473:2006 that are not fully satisfied and Certification to DD 245:2002 may continue up until 30th June 2007. Failure to satisfactorily address any non-compliances against BS 8473:2006 edition by 30th June 2007 will then impact upon the on-going approval decisions.

NOTE REGARDING THE STATUS OF BS 8473:2006: Although issued as a Code of Practice by British Standards Institution, it is important to note that compliance with the recommendations given is regarded as mandatory for all organisations wishing to maintain an NSI approval; subject to any additional clarifications and guidance included within this Technical Bulletin or issued subsequently. **The recommendations given in BS 8473:2006 should therefore be regarded as requirements of the appropriate NSI approval schemes.**

SUMMARY OF KEY CHANGES
(Highlighted under the clauses of the new Standard)

Comments under each clause consist of a summary of the changes introduced through BS 8473:2006 when compared with the corresponding clause within DD 245:2002.

Where the actual wording of the Standard is quoted it is reproduced in bold text.

Where it is considered relevant to further clarify the specified requirement, additional guidance is included in italics.

It is not the intent of NSI to impose its own recommended methods of compliance with specified requirements and NSI will give consideration to any alternative methods of achieving compliance with specified requirements.

A BRIEF SUMMARY OF THE CHANGES IS GIVEN IN THE ANNEX ATTACHED TO THIS TECHNICAL BULLETIN.

FOREWORD

The Foreword to BS 8473 now records that **'BS 8473 has been drawn up to assist all parties in the management of false alarms. False alarms are responsible for absorbing a disproportionate level of resources of the police, the alarm industry, clients and operators, and it is in the interests of those concerned that all parties seek to reduce their false alarms to a minimum.'**

1. SCOPE

The Scope now states **'This British Standard gives guidance on the management of intruder and hold-up alarm systems (I&HAS), and the management of alarm conditions when they occur in order to reduce the nuisance factor and waste of resources in responding to false alarms.**

'This document applies to all remotely notified intruder and hold-up alarm systems and also applies to audible only intruder and hold-up alarm systems, except where otherwise stated.'

BS 8473:2006 has adopted the terminology of the European Standard EN 50131 for intruder and hold-up alarm systems. However, BS 8473 also applies to intruder alarm systems installed to British Standards (e.g. BS 4737).

2. NORMATIVE REFERENCES

The Standard calls up **'PD 6662:2004, Scheme for the application of European Standards for intruder and hold-up alarm systems'** in place of PD 6662:2000.

The Standard calls up **'BS EN 50131-1:2006, Alarm systems – Intrusion systems – Part 1: System requirements'** in place of BS EN 50131-1:1997.

For the purposes of the relevant NSI schemes for approval, the provisions of PD 6662:2004 and the Standards called-up by PD 6662:2004, continue to apply. Therefore, until such time as PD 6662:2004 is amended or revised, prEN 50131-1:2004 continues to apply rather than BS EN 50131-1:2006.

The Standard calls up **'DD CLC/TS 50131-7, Alarm systems – Intrusion systems – Part 7: Application Guidelines'**.

The Standard calls up **'DD 243:2004, Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions – Code of practice'**.

3. TERMS AND DEFINITIONS

Changes to the definitions and also some of the more important definitions in the Standard are covered below.

3.5 alarm receiving centre-related false alarm

The Standard introduces a new definition **'false alarm attributable to a fault, failure, error, or omission on the part of the ARC responsible for monitoring the I&HAS'.**

Examples of ARC-related false alarms are given in Annex C of the Standard and include **'human error, policing a system while system is on test, failing to put system on test, policing unconfirmed alarms from confirmed systems, passing of incorrect information to police, ARC equipment failure'.**

The reasons that an ARC might pass an alarm to police when a system is on test are more likely to be due to misunderstandings between the ARC and the person putting the system on test rather than failing to put a system on test. This can include putting the wrong system on test (if there is more than one system at the supervised premises) or a misunderstanding about when the system is taken off test. These misunderstandings can be minimised though careful and close discussion between the parties.

Where a time period is agreed for the test, there is a risk that the time period might expire before the test is completed. Installation and service technicians should make sure that the arrangements with ARCs are such that either the test is completed before the time period expires or the time period is extended where necessary.

In order to minimize the occasions where unconfirmed alarms are passed incorrectly to police, ARCs need to be provided with the correct, up-to-date information. In the case where

an ARC calls police incorrectly and the reason is that the alarm company has failed to provide the ARC with the correct information, the cause of the false alarm should be recorded as a company-related false alarm.

3.6 client

The term 'client' is defined in the Standard as **'person or organisation utilizing the services of an alarm company for the installation and/or maintenance of an I&HAS'**. This is the term for the alarm company's customer, previously called the 'subscriber' in BS 4737.

3.8 false alarm

The term 'false alarm' is defined in the Standard as **'policed alarm condition other than a genuine alarm'.**

All 'policed alarm conditions' are false alarms unless they are genuine alarms according to the definition of 'genuine alarm'.

3.9 false alert

The term 'false alert' is defined in the Standard as **'remotely notified alarm condition, which is regarded by the ARC as cancelled, such cancellation having been authorised by the operator of the I&HAS'.** Further details are given in Notes in the Standard.

3.10 genuine alarm

The term 'genuine alarm' is defined in the Standard as **'policed alarm condition which has resulted from:**

a) a criminal attack, damage, or attempt at such, upon/to the supervised premises, the alarm equipment or the transmission path carrying the alarm signal; or

b) actions by emergency services in the execution of their duties; or

c) a call emanating from a hold-up alarm system made to summon urgent assistance when an assailant enters a previously defined area with the obvious intention of harming or threatening any person within that defined area'.

Annex E of the Standard gives guidelines to avoid false hold-up alarm activations.

3.12 operator

The term 'operator' is defined in the Standard as **'authorised individual using an I&HAS for its intended purpose'**. These are individuals authorised by the client (customer) to use/operate the I&HAS and can of course include the client himself/herself.

3.14 policed alarm condition

The term 'policed alarm condition' is defined in the Standard as **'remotely notified alarm condition which (after any defined time delay for completion of alarm filtering, if applicable) has not been classified as a false alert and which therefore has been duly extended to the police'.**

Where police are called in relation to a remotely notified unconfirmed alarm signal and a transmission path fault (see sub-clause 4.3 of DD 243:2004), the alarm signal must be regarded as a 'policed alarm condition' for the purpose of determining whether the RMC is permitted to 'restore' / 'reset' the I&HAS (see Clause 10 of BS 8473:2006).

Where police are called in relation to transmission path faults (i.e. from two paths of different technologies), police will categorise the call as either genuine or false. However, calls made to police solely in relation to transmission path faults are NOT regarded as 'policed alarm conditions' for the purpose of determining whether the RMC is permitted to 'restore' / 'reset' the I&HAS (see Clause 10 of BS 8473:2006).

3.16 remotely notified alarm condition

The term 'remotely notified alarm condition' is defined in the Standard as **'state of monitoring equipment at an ARC (or other remote location) which indicates an alarm condition'**. This definition replaces the definition of 'signalled alarm condition' given in DD 245:2002.

3.17 restore

The term 'restore' is defined in the Standard as **'procedure of cancelling an alarm, tamper, fault or other condition and returning the I&HAS to a previous condition.'**

There is a NOTE in the Standard that states **'This was previously known as "reset".'**

3.18 restore management centre (RMC)

The term 'restore management centre' is defined as **'premises where the authorisation of the restoring of a remotely notified I&HAS is permitted'.** The similar definition given in DD 245 was called 'reset management centre'.

3.21 unconfirmed alarm

The term 'unconfirmed alarm' is defined as **'signal that has not been designated as audibly confirmed, visually confirmed or sequentially confirmed'.**

An 'unconfirmed alarm' becomes a 'false alert' if an operator of the I&HAS authorises the ARC to cancel the alarm (for example by causing an unset signal or a mis-operation signal to be transmitted to the ARC).

4. SYSTEM DESIGN

The Standard states **'Further guidance to assist in designing systems for minimization of false alarms is given in DD 243.**

There is also a NOTE in the Standard that states **'DD CLC/TS 50131-7 gives guidance for good system design practice.'**

5. ADMINISTRATION

The content of Annex E of DD 245:2002 has been transferred to Clause 5 of BS 8473:2006 and the wording has been improved/revised.

5.1 General

The Standard now states **'Each alarm company should appoint a person within the company who is responsible for the performance if intruder and hold-up alarm systems (I&HAS). The appointed person should have the right of direct access to the Chief Executive/Managing Director and have sufficient experience and authority within the company to achieve the objectives of monitoring, analysing and reducing false alarms. In the case of a small company, the Chief Executive/Managing Director may personally undertake this role.**

NOTE 1 **In this Code of Practice the appointed person is referred to as the Systems Performance Manager (SPM).**

NOTE 2 **Depending upon the size and regional distribution of the company, it might be necessary to appoint regional managers having corresponding responsibility for the performance of I&HASs within particular regions and reporting to the SPM.**

5.2 Functions of Systems Performance Manager (SPM)

The responsibilities of an SPM are defined in sub-clause 5.2. '**The SPM should ensure that the following tasks are carried out effectively in the alarm company:**

a) Monitoring of the standards of surveying and installation to ensure that:

1) industry standards and codes of practice are complied with;

2) system design proposals meet the requirements of the alarm company's policies;

3) system design proposals do not result in systems which are likely to generate false alarms;

4) client documentation is provided in accordance with DD CLC/TS 50131-7 and DD 243;

5) comprehensive training for alarm company staff is maintained;

6) training for operators is provided in accordance with DD CLC/TS 50131-7.

b) Maintenance of all contracted systems at intervals in accordance with PD 6662. Training for operators should be offered at each site visit.

NOTE Systems installed in accordance with BS 4737 are maintained at intervals specified in BS 4737-4.2.

c) Monitoring of demands for and effectiveness of corrective maintenance in accordance with PD 6662.

NOTE Systems installed in accordance with BS 4737 are maintained at intervals specified in BS 4737-4.2.

d) Identification of abnormalities and trends likely to lead to false alarms.

e) Monitoring of the alarm company's false alarm management procedure (see Clause 8).

1) Collection, reporting and analysis of false alarm statistics and their causes.

2) Identification of troublesome systems, equipment and practices.

3) Identification of transmission path problems.

f) Monitoring of client complaints.

g) Monitoring liaison with police security systems offices and maintaining familiarity with their policies.

h) Monitoring evaluation trials on new equipment, with particular reference to false alarms.

i) Ensuring compliance with this British Standard.

j) Working with operational management to obtain a reduction in the incidence of false alarms.'

BSI is developing DD 263 for commissioning and maintenance of intruder and hold-up alarms. In due course, the maintenance provisions of DD 263 are likely to replace those of BS 4737-4.2 in the UK.

5.3 Checklist of Points for Preventing False Alarms

The Standard states that **'Alarm companies should pass the information given in Annex D and Annex E to clients to aid in the prevention of operator-related false alarms.'**

Annex D of BS 8473 gives 11 points to remember in terms of preventing false alarms. The eleventh point is new and states **'Most IAS require a mains electricity supply. If the electricity supply to your system is disconnected for more than 4 h contact the alarm company.'**

Annex E of BS 8473 is new and includes guidance on how to avoid false hold-up alarms.

6 DOCUMENTATION AND TRAINING

6.1 This sub-clause has been strengthened through the statement that **'the alarm company should provide the client representative(s) with sufficient written instructions, reinforced by adequate training, to ensure correct operation can be achieved.'**

Also, there is a NOTE in the Standard that states **'The client is responsible for ensuring that only competent operators are permitted to use the I&HAS.'**

6.2 This sub-clause states that **'Annex F gives an example of a typical corrective maintenance report form. The completed document should be copied to the client.'**

It is still important that the prime cause of a false alarm is established and recorded in the corrective maintenance report. The Standard states that **'The company-wide standard categorization of alarm activations in accordance with Annex G should be used on the corrective maintenance report form.'**

Annex G gives the following categorizations as a minimum: genuine alarm; company-related alarm; operator-related alarm; ARC-related alarm; transmission path fault-related alarm; cause-unknown alarm.

Every attempt should be made to ascertain the cause of false alarms in order to minimize the number of alarms categorized as cause-unknown. Further subdivision can be useful for the alarm company's own purposes and analysis; additional forms of categorisation (e.g. by age of system) can yield useful information.

6.3 Sub-clause 6.3 c) and 6.3 d) in DD 245:2002 have been merged into sub-clause 6.3 c) in the new standard.

Sub-clause 6.3 c) of BS 8473 recommends that the system of monitoring all remotely notified alarm conditions needs to **'provide a register of all remotely notified alarm conditions and of all other conditions (e.g. local audible) that have been reported to the alarm company, and discriminate between genuine alarms, false alarms, unconfirmed alarms, and false alerts for monthly analysis.'**

There is still a requirement to provide an analysis of monthly alarm condition statistics. The change in the Standard is to discriminate between 'unconfirmed alarms' and 'false alerts', as well as 'genuine alarms' and 'false alarms'.

7 STATISTICS RELATING TO REMOTELY NOTIFIED I&HAS

The Standard states **'An alarm company should compile and collate a record of all remotely notified alarm conditions it receives as follows:**

a) Details of all remotely notified alarm conditions should be recorded and categorized as either genuine alarms under several different parameters, unconfirmed alarms, false alarms, or false alerts.

The wording of 7 a) of the Standard is a little unclear and it is helpful to re-express the recommendation as follows:

Details of all remotely notified alarm conditions should be recorded and categorized (i) as genuine alarms, (ii) under several different parameters as false alarms, (iii) as unconfirmed alarms, and (iv) as false alerts.

The main change is the addition of unconfirmed alarms into the categorization. An 'unconfirmed alarm' (see definition 3.21) is a type of remotely notified alarm condition (i.e. not designated as confirmed) whereas a 'false alert' (see definition 3.9) is a remotely notified alarm condition that is regarded by the ARC as cancelled, such cancellation having been authorised by the operator of the I&HAS.

An 'unconfirmed alarm' should not be passed to the police, and then if it is not cancelled by the operator of the I&HAS it remains an 'unconfirmed alarm'.

Any 'remotely notified alarm condition' that is cancelled by the operator of the I&HAS without being passed to the police is a 'false alert'.

Any 'remotely notified alarm condition' that is passed to the police becomes a 'policed alarm condition' and then it either becomes a 'genuine alarm' or a 'false alarm'.

b) Monthly alarm reports should be compiled on an overall company basis, and for each office (see 6.3), including categorization under appropriate categories (see Annex C), so that common problems can be identified.

There is no change to the Standard other than inclusion of the reference to Annex C, which gives examples of company-related false alarms, operator-related false alarms and ARC-related false alarms.

It is not a requirement to categorise strictly in accordance with Annex C. However, the categorisation should be adequate enough to identify common problems. There may be other causes of false alarms that are not included in Annex C.

c) Figures from the monthly reports should be included in a rolling 12-monthly log, so that a long-term analysis can be made of unconfirmed alarms, false alarms and false alerts.

The change to the Standard is that unconfirmed alarms and false alerts have now been included in sub-clause 7 c) along with false alarms.

Figure G.2 of Annex G provides a model form for recording remotely notified alarm conditions that leads to a rolling 12-monthly log of "policed" false alarms.

It is not intended that there needs to be a rolling 12-monthly log of unconfirmed alarms or a rolling 12-monthly log of false alerts according to the methodology given in Figure G.2 of Annex G for "policed" false alarms. However, monthly figures (totals) for unconfirmed alarms and for false alerts need to be included with the rolling

12-monthly log of false alarms so as to assist in the long-term analysis of the causes of false alarms.

Increases in the numbers of unconfirmed alarms and/or false alerts may increase the likelihood of false alarms if the causes of these unconfirmed alarms and/or false alerts are not identified and addressed with clients.

d) Company-wide statistics should be compiled, as well as statistics relating to each office. Each office should retain copies of the statistics relating to its own area of responsibility which should be made available for inspection.

Apart from minor changes to the wording, this sub-clause of the Standard has not changed.

e) The SPM should oversee the production of the monthly and rolling 12-monthly analyses and ensure that the information is sent to senior executives and others within the alarm company, as appropriate.

Apart from minor changes to the wording, this sub-clause of the Standard has not changed.

8 FALSE ALARM MANAGEMENT PROCEDURE

This clause has been strengthened. **'Alarm companies should have a documented process by which the occurrence of false alarms, unconfirmed alarms, and false alerts is identified.'**

This process should include a means by which **'any installation giving rise to a false alarm, or more than three unconfirmed alarms and/or false alerts in a rolling 30 day period is identified and reported to the appropriate levels of management for information and action. The aim of the false alarm management procedure is to identify troublesome installations and to overcome the problem before police response is withdrawn.'**

9 DIAGNOSIS OF FALSE ALARMS

There is no change to the Standard except for the final sentence which now reads **'This training should be documented and the records retained'.**

10 RESTORING OF REMOTE NOTIFICATION I&HASs CAPABLE OF POLICED ALARM CONDITIONS

Editorially there has been some re-organisation of the content of Clause 10 of BS 8473: 2006, compared with DD 245:2002, and the sub-clauses of BS 8473 have been given sub-titles.

The principles of Clause 10 of BS 8473:2006 are as follows:

a) There are circumstances where the I&HAS needs to be configured such that the customer is denied the facility to set or restore (reset) the I&HAS (see sub-clause

10.1 of the Standard). In these circumstances the customer has to request a restore (reset) from the alarm company or from a Restore Management Centre.

b) The types of premises that are permitted as Restore Management Centres (RMCs) are limited (see sub-clause 10.2 of the Standard).

c) Where the customer is denied the facility to set or restore (reset) the I&HAS, there are only certain permitted ways in which the I&HAS can be restored (see sub-clause 10.3 of the Standard).

d) There are certain conditions that must be satisfied before an RMC can authorise the restore (reset) of an I&HAS after a 'policed alarm condition' has occurred (see sub-clause 10.4 of the Standard – see also item g) below). If these conditions are not satisfied, the alarm company's service technician needs to attend the supervised premises to restore (reset) the I&HAS.

e) ARCs must maintain certain records and ARCs have a duty to inform alarm companies of remotely notified alarm conditions (see sub-clause 10.5 of the Standard).

f) There are matters affecting the inter-relationship between the RMC and the ARC when the RMC is not an ARC (see sub-clause 10.6 of the Standard).

g) The RMC must deny restore (reset) in relation to a 'policed alarm condition' if one or more 'policed alarm conditions' have previously occurred in the last 12 months (see sub-clause 10.7 of the Standard). Then the alarm company's service technician needs to attend the supervised premises to restore (reset) the I&HAS.

The RMC may authorise restore (reset) if the new 'policed alarm condition' is a genuine alarm. However, this is subject to a condition (see sub-clause 10.7 of the Standard).

h) There are certain conditions that must be satisfied before the RMC can authorise the restore (reset) of an I&HAS in accordance with sub-clause 10.3 b) after a 'false alert' has occurred (see sub-clause 10.8 of the Standard). If these conditions are not satisfied, the alarm company's service technician needs to attend the supervised premises to restore (reset) the I&HAS.

i) There are certain conditions that must be satisfied before the RMC can authorise the restore (reset) of an I&HAS in accordance with sub-clause 10.3 c) after a 'false alert' has occurred (see sub-clause 10.9 of the Standard). If these conditions are not satisfied, the alarm company's service technician needs to attend the supervised premises to restore (reset) the I&HAS.

For further details please refer to Clause 10 of BS 8473:2006 and the information and guidance given below in this Technical Bulletin.

10.1 I&HAS Configuration

This sub-clause gives the circumstances under which the customer (i.e. the client and/or owner and/or operator of the I&HAS) is denied the facility to set or restore (reset) the I&HAS. The customer can then only set the I&HAS after the I&HAS has been restored (reset) in accordance with the methods given in sub-clause 10.3.

The Standard states that **'The I&HAS should be configured so that the client and/or owner and/or operator is unable to set or restore the I&HAS after the following conditions have occurred.'**

- **'In the case of I&HASs conforming to DD 243:2002 or subsequent editions of DD 243; a sequentially confirmed alarm condition.'**

  This provision denies the customer the facility to "reset" an intruder alarm system complying with BS 4737 and DD 243 after a sequentially confirmed alarm has occurred. It represents no change to the existing position under BS 4737.

  This provision also denies the customer the facility to restore (reset) an intruder alarm system complying with PD 6662 / EN 50131 and DD 243 after a sequentially confirmed alarm has occurred. This is a change to the Standard compared with sub-clause 10.1 of DD 245:2002.

  After a sequentially confirmed alarm has been remotely notified, the Control and Indicating Equipment (CIE) does not know whether the alarm will be cancelled by an operator of the system or be passed to the police. Even where an alarm is cancelled, it may be too late to stop the police being called. Therefore, CIE needs to be configured so that a restore (reset) is always required after a sequentially confirmed alarm has occurred.

  If an unconfirmed alarm occurs the customer (client / owner / operator) is permitted to restore (reset) the system. This applies irrespective of whether or not the unconfirmed alarm is subsequently designated at the ARC as audibly confirmed or as visibly confirmed.

- **'In the case of I&HASs conforming to a standard that pre-dates DD 243:2002; an intruder alarm condition.'**

  This provision denies the customer the facility to restore (reset) an intruder alarm system complying with BS 4737 after an intruder alarm condition has occurred. It represents no change to the existing position under BS 4737.

  In the case of a so-called 'legacy system' on police response that complies with BS 4737, but does not incorporate alarm confirmation technology, the control panel needs to be reset after an intruder alarm has occurred.

- **'In the case of I&HASs conforming to PD 6662:2004 at grade 3 or 4; a tamper condition.'**

This provision denies the customer the facility to restore an intruder alarm system complying with Grade 3 or Grade 4 of PD 6662:2004 (or later edition) after a tamper alarm condition has occurred. This is a new requirement.

10.2 Restore Management Centres (RMCs)

This sub-clause determines the types of premises that are permitted as RMCs. There are no significant changes to the Standard compared with sub-clause 10.2 of DD 245: 2002.

10.3 Methods of Restoring

This sub-clause gives the methods of restoring (resetting) an I&HAS when the customer is denied the facility to restore (reset) according to sub-clause 10.1.

There are no significant changes to the methods of restoring (resetting). For ease of reference, restoring of the conditions defined in 10.1 can only be carried out:

a) 'by the alarm company's service technician at the supervised premises;

b) 'by the operator at the supervised premises, acting in conjunction with the RMC and authorised by the RMC, in accordance with 10.4, 10.8 and 10.9;

An example would involve the use of an anti-code generator.

c) 'Remotely by means of electronic signals transmitted from the RMC (the RMC acting in conjunction with the operator in attendance at the supervised premises) and authorized by the duty officer at the RMC, in accordance with 10.4, 10.8 and 10.9.'

There is a new recommendation, which is that **'Codes used by the alarm company service technician for maintenance and testing purposes should not be disclosed to the operator.'**

The recommendation in sub-clause 10.3 of BS 8473:2006, which is similar to the recommendation given in sub-clause 10.11 of DD 245:2002, reads **'In the case of 10.3b) and 10.3c), the method of restoring the I&HAS should be such that the RMC is able to determine whether the ATS is restored or not.'**

IN THE ABOVE RECOMMENDATION THERE IS AN ERROR IN THE STANDARD AND THE ABBREVIATION 'ATS' SHOULD READ 'I&HAS'.

10.4 Restoring of Policed Alarm Conditions

This sub-clause gives the conditions that must be satisfied before the RMC can authorise the restore (reset) of an I&HAS after a 'policed alarm condition' has occurred. They are similar to the conditions given in sub-clause 10.7 of DD 245: 2002.

10.5 ARC Record of Remotely Notified Alarm Conditions

The recommendations given in this sub-clause of BS 8473:2006 are similar to those given in sub-clause 10.8 and sub-clause 10.16 of DD 245:2002. They relate to the records that must be maintained by ARCs and to the duty of ARCs to inform alarm companies of remotely notified alarm conditions.

10.6 Inter-Relationship Between the RMC and the ARC

The recommendations given in this sub-clause of BS 8473:2006 are similar to those given in sub-clause 10.9, sub-clause 10.10 and sub-clause 10.12 of DD 245:2002. They relate to matters affecting the inter-relationship between the RMC and the ARC where the RMC is not itself an ARC.

10.7 RMC Policy of Denying Restore

This sub-clause gives the RMC (ARC) policy of denying restore (reset) in relation to 'policed alarm conditions'.

There has been a SIGNIFICANT CHANGE compared with sub-clause 10.13 of DD 245:2002). The Standard states that **'The RMC should deny restore if more than one policed alarm condition has occurred in the last 12 months.'**

'When the RMC denies a restore, the alarm company's service technician should visit the supervised premises for the purpose of identifying the cause of the alarm condition, carrying out corrective maintenance/action and ensuring that the I&HAS is in full working order and,

a) in the case of a false alarm due to operator error, educating the operator in the operation of the I&HAS, and the avoidance of false alarms. See Annex D;

b) if design faults are noted these are reported to the SPM (see 5.2) by the next working day.'

However, the RMC may authorise restore (reset) of the I&HAS if the new 'policed alarm condition' is a genuine alarm subject to the following condition:

'The RMC may permit a restore if a genuine alarm, or genuine confirmed alarm, has occurred provided the RMC always advises the operator that insurance cover could be invalidated if a service technician's visit does not take place and the I&HAS is subsequently found not to be in full working order.'

10.8 Restoring of False Alerts

This sub-clause gives the conditions that must be satisfied before the RMC can authorise the restore (reset) of an I&HAS in accordance with sub-clause 10.3 b) after

a 'false alert' has occurred. They are similar to the conditions given in sub-clause 10.14 of DD 245: 2002.

Provided all the conditions are satisfied, there is no limit to the number of restores (resets) that can be authorised by the RMC after a 'false alert' has occurred.
However, there is a strict limit on the number of restores (resets) that can be authorised after a 'policed alarm condition' has occurred (see 10.7 above).

10.9 Restoring of False Alerts Remotely by the RMC

This sub-clause gives the conditions that must be satisfied before the RMC can authorise the restore (reset) of an I&HAS in accordance with sub-clause 10.3 c) after a 'false alert' has occurred. They are similar to the conditions given in sub-clause 10.15 of DD 245: 2002.

Annex A (Informative)
Typical Steps in the Transmission and Filtering of Alarm Conditions

The recommendations given in Annex A of BS 8473:2006 are similar to those given in Annex A of DD 245:2002.

Annex B (Informative)
Progress of an Alarm Condition

The recommendations given in Annex B of BS 8473:2006 are similar to those given in Annex B of DD 245:2002 except that Annex B of BS 8473:2006 includes two Figures, B.1 and B.2, one relating to I&HAS not capable of generating confirmed alarms, the other relating to I&HAS capable of generating confirmed alarms.

Unfortunately, the headings for Figures B.1 and B.2 were the wrong way round. However, BSI has corrected his by publishing Corrigendum No. 1 to BS 8473:2006.

Annex C (Informative)
Examples of False Alarms

The recommendations given in Annex C of BS 8473:2006 are similar to those given in Annex C of DD 245:2002 except for the addition of C.3 relating to ARC-related false alarms.

Annex D (Normative)
Preventing False Alarms: Points to Remember

The recommendations given in Annex D of BS 8473:2006 are similar to those given in Annex F of DD 245:2002 except for the addition of an additional point to remember given in D.11, which is that:

'Most IAS require a mains electricity supply. If the electricity supply to your system is disconnected for more than 4 h contact the alarm company.'

Annex E (Normative)
Hold-Up Alarms

Annex E of BS 8473:2006 is new and includes guidelines to avoid false activations of hold-up devices.

Annex F (Informative)
Corrective Maintenance Report Form

Annex F of BS 8473:2006 contains a model form for recording corrective maintenance that is similar to the model form given in Annex G of DD 245:2002.

Annex G (Normative)
Recommendations for the Recording of Remotely Notified Alarm Conditions

The recommendations given in Annex G of BS 8473:2006 are similar to those given in Annex H of DD 245:2002.

However, Annex G of BS 8473:2006 re-introduces a model form (see Figure G.2) for recording remotely signalled/notified alarm conditions, which is a revised version of the model form given in NSI/NACOSS Code of Practice NACP 10 (Issue 2).

The model form in Figure G.2 is intended for remote signalling/notification alarm systems on police response.

THERE IS AN ERROR IN FIGURE G.2. THE ROWS LABELLED ‘O’ AND ‘P’ SHOULD BE COMBINED INTO ONE ROW LABELLED ‘P’ AND THE LABEL ‘O’ SHOULD NOT EXIST.

The rolling 12-monthly analysis of false alarms for remote signalling systems on police response can be carried for all remote signalling systems on police response without needing separate analyses (i) for systems incorporating alarm confirmation technology and (ii) for systems not incorporating alarm confirmation technology. It is of course perfectly satisfactory for alarm companies to perform separate analyses if they prefer.

Annex H (Normative)
Attendance on False Alarms

The recommendations given in Annex H of BS 8473:2006 are similar to those given in Annex J of DD 245:2002. However, they have been simplified in recognition of the reduction in the number of false alarms that can occur before police response is withdrawn.

ANNEX

BRIEF SUMMARY OF CHANGES

1. *Each alarm company must appoint a person within the company who is responsible for the performance of intruder and hold-up alarm systems (I&HAS). The appointed person must have the right of direct access to the Chief Executive/Managing Director and have sufficient experience and authority within the company to achieve the objectives of monitoring, analysing and reducing false alarms. The appointed person is referred to as the Systems Performance Manager (SPM) and in a small company the Chief Executive/Managing Director may personally undertake this role. The responsibilities of the SPM are given in sub-clause 5.2 of the Standard.*

2. *The SPM must oversee the production of the monthly and rolling 12-monthly analyses of false alarms and must ensure that the information is sent to senior executives and others within the alarm company, as appropriate.*

3. *Any installation giving rise to a false alarm, or more than three unconfirmed alarms and/or false alerts in a rolling 30 day period must be identified and reported to the appropriate levels of management for information and action.*

4. *The alarm company must provide the client representative(s) with sufficient written instructions, reinforced by adequate training, to ensure correct operation of the I&HAS can be achieved.*

5. *Alarm companies must discriminate between genuine alarms, false alarms, unconfirmed alarms, and false alerts in the register of alarm conditions (see sub-clause 6.3c) of the Standard).*

6. *Alarm companies must include ARC-related false alarms in the categorization of alarms. Every attempt should be made to ascertain the cause of false alarms in order to minimize the number of alarms categorized as cause-unknown.*

7. *The I&HAS must be configured so that the client and/or owner and/or operator is unable to set or restore (reset) the I&HAS after the following conditions have occurred:*

    - *In the case of I&HASs conforming to DD 243:2002 or subsequent editions of DD 243; a sequentially confirmed alarm condition.*

    - *In the case of I&HASs conforming to a standard that predates DD 243:2002; an intruder alarm condition.*

    - *In the case of I&HASs conforming to PD 6662:2004 at grade 3 or 4; a tamper condition.*

8. *Codes used by the alarm company service technician for maintenance and testing purposes must not be disclosed to the operator.*

9. The RMC must deny restore (reset) if more than one policed alarm condition has occurred in the last 12 months.

10. The RMC may permit a restore (reset) if a genuine alarm, or genuine confirmed alarm, has occurred provided the RMC always advises the operator that insurance cover could be invalidated if a service technician's visit does not take place and the I&HAS is subsequently found not to be in full working order.

11. When the RMC denies a restore (reset), the alarm company's service technician must visit the supervised premises for the purpose of identifying the cause of the alarm condition, carrying out corrective maintenance/action and ensuring that the I&HAS is in full working order and,

a) In the case of a false alarm due to operator error, educating the operator in the operation of the I&HAS, and the avoidance of false alarms.

b) If design faults are noted, must report these to the SPM by the next working day.

****