National Security Inspectorate
Sentinel House
5 Reform Road
Maidenhead
SL6 8BY UK

T +44 (0)1628 637512
F +44 (0)1628 773367
E nsi@nsi.org.uk
W nsi.org.uk

AWEW/mjc/NSI 012/15 21 July 2015

To: All NSI NACOSS Gold Approved Companies, NSI Systems Silver Approved Companies and NSI ARC Gold Approved Companies and Applicants

Dear Colleague

IA 1501:2015 INDUSTRY AGREEMENT ON INTERIM UPDATE OF PD 6662:2010

Please find attached an Industry Agreement, which provides an interim update to PD 6662:2010 pending a revision of PD 6662 via British Standards Institution.

Your audits will include the revised requirements with effect from 1 September 2015 and from this date your system design proposals and as-fitted documents must state that I&HASs conform to PD 6662:2010 + IA 1501:2015.

The agreement brings PD 6662 into line with changes to other standards including BS 8243, BS 8473 and DD CLC/TS 50131-7. We have adopted Amendment 1 to BS 8243:2010 already via our circular letter (Ref: AWEW/mjc/NSI 007/14) dated 24 June 2014.

We will provide you with further information about the changes to BS 8473 relating to management of false alarms, which are relatively straightforward.

PD 6662:2010 contains statements relating to DD CLC/TS 50131-7:2008, which were resolved when DD CLC/TS 50131-7:2010 was published. Therefore adopting the 2010 edition of DD CLC/TS 50131-7 does not involve any significant changes.

The agreement allows you to continue using vibration detectors complying with BS 4737-3.10:1978 or you can use vibration (shock) detectors complying with PD CLC/TS 50131-2-8:2012. However you must hold evidence of compliance to the relevant standards.

Under the agreement you must use cable complying with BS 4737-3.30:2015 (which is a new cable standard) for contracts entered into from 1 April 2016 including new work involving cabling on existing systems.

Contd/…

The agreement allows your customers to use remote devices (such as smart phones) to operate intruder alarm systems subject to compliance with the Industry Agreement. The provision of remote devices is optional and will depend on your customers' needs. If you choose to offer remote devices you must hold evidence of compliance to Annex C of BS EN 50131-3:2009 from the manufacturers in line with the Agreement. Some further information is provided in the Annex attached to this letter.

We would appreciate any feedback about the agreement to feed into the revision of PD 6662 and please do not hesitate to contact me at email tony.weeks@nsi.org.uk if you have any questions.

Yours sincerely

Tony Weeks
Head of Technical Services

Att.

ANNEX

FURTHER INFORMATION ABOUT THE USE OF REMOTE DEVICES TO OPERATE INTRUDER ALARM SYSTEMS

It is important to inform your customers about the potential issues involved in using remote devices. Used responsibly they can be a valuable asset to the user. However difficulties can occur.

It is possible, for example, that low battery at the remote device and/or poor or intermittent communications could lead to situations where users have initiated setting or unsetting and are unable to verify, at least for a period of time, whether the action was successful or not.

You should therefore brief customers in writing on these particular risks and advise them where possible to avoid using remote devices where there are signal strength issues or when the device battery is low.

False alarms

There is a potential risk of false alarms from the use of remote devices, for example if people are inadvertently still inside the supervised premises when the intruder alarm system is set. Therefore please keep separate records of any false alarms from remote devices and handle them in accordance with BS 8473 with the objective of keeping false alarms to a minimum.

Security issues

Using a remote device to unset the intruder alarm system risks the premises being occupied for a period of time. According to the industry agreement, a warning in **bold type** must be included in the system design proposal and as-fitted document as follows:

> **IMPORTANT**
>
> **If using a device to remotely set/unset your intruder alarm system, your attention is drawn to the fact that whenever a premises is unattended but its intruder alarm system(s) is (are) not fully set, any related insurance cover might be inoperative. For advice on this matter, it is recommended that you consult your insurer(s).**

The theft of a remote device could potentially compromise the intruder alarm system. However applications used on remote devices must incorporate a security code that meets the authorisation requirements of BS EN 50131-1 (for example 10,000 differs in Grade 2) and is independent of security functions associated with unlocking the device itself, which could be disabled by the user.

ANNEX (CONTINUED)

FURTHER INFORMATION ABOUT THE USE OF REMOTE DEVICES TO OPERATE INTRUDER ALARM SYSTEMS

It is unlikely that an application would incorporate a “remember me” facility to overcome the need to enter an authorisation code each time the application is used. However customers should be advised not to implement such a facility, if it exists, for security reasons.

More likely a thief might attempt to work through the security codes to find one that succeeds in which case a lockout after a given number of false code entry attempts would be useful.

You should also check that all communications between the user’s remote device and the intruder alarm system will be encrypted using a publicly available encryption scheme.