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

MH/LW/NSI 019 20 06 May 2020

To: All NACOSS Gold, Systems Silver, Fire Gold and Fire Silver approved companies and applicants

Dear Colleague,

- YOUR INVITATION TO COMMENT -

NEW DRAFT 'CYBER SECURITY FOR INSTALLERS' CODE OF PRACTICE: THE BASIS OF A FUTURE NSI SCOPE WITHIN NACOSS GOLD/SYSTEMS SILVER/ FIRE GOLD/FIRE SILVER APPROVAL

This letter is to invite you to participate in commenting on the final drafting of the BSIA's NEW DRAFT 'CYBER SECURITY FOR INSTALLERS' Code of Practice on/before 19th May 2020.

NSI has been working in conjunction with the BSIA and other industry parties in developing a Cyber Security Code of Practice for Installers of electronic security systems, with the view to incorporating it within NSI NACOSS Gold, Systems Silver, Fire Gold and Fire Silver Schemes in due course.

The demands on installers are ever increasing in terms of technical competencies required to install systems, often with internet connectivity, in cyber secure fashion. This draft Code is designed to assist installers in building and maintaining competency. It is envisaged the Code will in due course strengthen the standing of your NSI approval in the marketplace.

NSI is committed to supporting this initiative and trust you will consider the opportunity to provide your input to the Code. See the Appendix below for more details.

If you would like to participate in a virtual meeting where I will present the Code as it could apply to NSI approved companies, please register your interest ASAP with my colleague, Gayle Bennett (gayle.bennett@nsi.org.uk) and you will receive an invitation to the presentation planned for 2pm on 13th May 2020.

Yours sincerely,

Matthew Holliday
Technical Manager
DDI: 01628 764862
Email: matthew.holliday@nsi.org.uk

APPENDIX

Background

The risk of cyber-attack in everyday life is becoming increasingly more prevalent. As more and more electronic devices are connected to the internet the need for cyber security also increases.

This risk translates into a need to protect service providers, organisations and the public from cyber-attack in the electronic security and fire protection industries. Time is approaching where there will be demand for evidence that organisations and their products are protected against cyber-attack. It is recognised there are a number of standards and certification schemes in existence today that can be adopted by organisations to evidence their cyber security credentials e.g. Cyber Essentials or Cyber Essentials Plus. A cross-industry group representing the electronic security and fire detection industry has developed a Code of Practice over the last couple of years aimed specifically at cyber security for security and fire detection systems. This cross industry group (CySPAG (Cyber Security Product Assurance Group)) has been led by the BSIA who will be publishing a Code of Practice later this year and making it freely available to everybody.

NSI expects to be offering optional cyber security certification scopes initially, at some point in the next couple of years. The BSIA Form 342 'Installation of Safety and Security Systems - Cyber Security Code of Practice' will form the basis for the NSI scopes, covering cyber security for installations. At some point this scheme is likely to become mandatory for NACOSS Gold and Fire Gold approval.

The BSIA Form 342 'Installation of safety and security systems - Cyber Security Code of Practice' developed by CySPAG is now in the pre-publication phase of 'public comment', where an opportunity exists to comment on the document which will be considered by CySPAG.

We invite you to take this opportunity and submit comments to influence the final Code of Practice. All comments must be submitted to matthew.holliday@nsi.org.uk by close of play on the 19th of May 2020.

When completing the comment form please be sure to include your proposed changes as well as your comments, as the CySPAG group will reject comments without a proposed change.

About the BSIA form 342 'Installation of safety and security systems - Cyber Security Code of Practice'

This has been developed by the Cyber interest group, CySPAG, which is made up of members of the BSIA and many other industry experts and stakeholders.

This Code of Practice is based on international industry best practice regarding cyber security and refers to recognised guidance and standards as it applies to safety and security systems.

It is intended this Code of Practice will assist in providing confidence throughout the supply chain, promoting secure connection of products and services, and delivering client assurance regarding connected solutions.

This Code of Practice aims to minimise the exposure to digital sabotage of installed devices, applications and systems with a cyber exposure for the protection of safety and security. It provides recommendations on the design, planning, operation, installation, commissioning and maintenance of installed devices, applications and systems with a cyber exposure.

This Code of Practice is intended to be used by organisations and stakeholders involved in the installation, commissioning, maintenance, and inspection of such systems and also by end users and those involved in remotely monitoring such systems.

This is your opportunity to influence standards in your industry and deals with the use of new technology not currently included in existing industry standards - please take this opportunity to provide some feedback.

Questions or Queries?

If you have any questions or queries regarding the implementation of the new requirements, please do not hesitate to contact me.

Attachments

- 'BSIA_Form_342_Cyber_Security_Installers_Form-Comments.pdf': Comment template form
- 'Draft Code of Practice'