

BSIA cyber exposure mitigation code of practice released

1 year ago



The BSIA has updated its manufacturers' code of practice that recommends on the design, testing and manufacture of safety and security products with a cyber exposure, whilst aligning with major new UK legislation.

Manufacturers of safety and security systems Cybersecurity code of practice, is based on international industry best practice regarding cybersecurity and refers to recognised guidance and standards applied to safety and security systems. Crucially, it aligns with UK's consumer connectable product security regime, the UK Product Security and Telecommunications Infrastructure (PSTI) Act: 2022, which came into effect this week for Relevant Connectable Products. A previous iteration of this code of practice was released 2021 already encompassing many of the key requirements of the Act and in many aspects going beyond them.

The code of practice, which underpins the BSIA manufacturers cyber assurance registration scheme, will assist in providing confidence throughout the supply chain promoting secure connection of products and services. Its aim is to deliver client assurance regarding connected solutions, assisting the supply chain in their duty of care to other network users, particularly with respect to protecting the integrity of existing cybersecurity countermeasures or the implementation of such countermeasures in new solutions.

Graham Evans, Technical Officer, BSIA, said: 'We are pleased to announce the release of our updated issue of the Manufacturers of safety and security systems Cybersecurity code of practice, incorporating the relevant references to the UK Product Security and Telecommunications Infrastructure (PSTI) Act: 2022.

"Alignment of our code of practice to the Act is of major importance and once again demonstrates the forward thinking of our members to ensure their products and services keep pace with the latest security standards and legislation."

Glenn Foot, Chairman, BSIA Cybersecurity Product Assurance Group (CySPAG), said: "The PSTI Act is a welcome addition to the world of cybersecurity, but it must be noted that it only covers the basics, and

there are likely to be additional requirements in the future.

“Cyber responsible manufacturers should be striving to exceed these minimum requirements in order to give their customers the highest level of confidence in relation to cyber security. To support manufacturers in exceeding the PSTI requirements, the CySPAG scheme provides guidance on best practices and recognition for manufacturers for going beyond the bare minimum for Cyber Security.”

Manufacturers of safety and security systems Cybersecurity code of practice, is available via the [CySPAG website](#).

Details on how to join the CySPAG registration scheme can be found on the registration page.