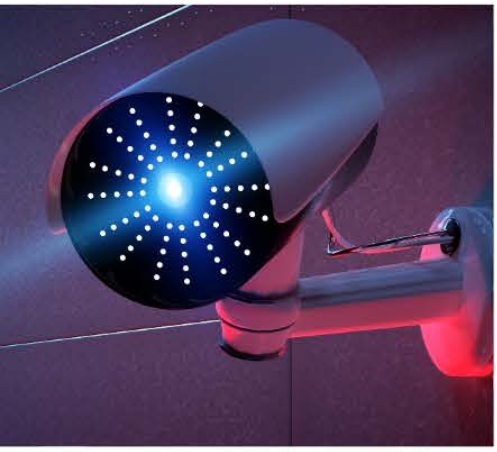


Security Suppliers PSTI Act

Compliance Guide

THE VOICE OF THE **PROFESSIONAL SECURITY INDUSTRY**

bsia
british security industry association

Contents

1. Overview

The document is designed to support businesses in the supply chain, which would include manufacturers, importers, and distributors, in dealing with the specifics of PSTI outlined in the scope of this document.

2. Scope of the PSTI Act

The PSTI Act received Royal Assent on the 6th December 2022. The Government published a full draft of the PSTI (Security Requirements for Relevant Connectable Products) Regulations in April 2023, and these regulations were signed into law on 14 September 2023. Compliance lies with the manufacturers, distributors and importers.

The UK's product security regulation has now come into force as of the 29th of April 2024 and is being enforced by the OPSS' Office for Products Safety and Standards regulatory authority.

It incorporates a wide range (non-exhaustive) list of consumer-connectable IOT products, for example: door-locks, alarm systems, smart doorbells, surveillance cameras, etc, that are connected to the internet or network by either LAN or WAN-based systems.

Excepted (exempt) connectable products are listed in Schedule 3 of the legislation.

The PSTI plays a crucial role in supporting the roll-out of future-proof gigabit broadband and 5G networks across the UK. By setting standards and requirements for product security, the Act is designed to safeguard critical infrastructure and protect consumers from cyber security risks.

For further information outside the scope of this document, please refer to the PSTI Regulation.

Please note that this guide is limited to the following:

- PSTI ACT and its Regulation – specific points for manufacturers have been highlighted.
- Basic idea and purpose of the Act.
- An example of compliance and non-compliance.
- Distributor and Importer definitions.
- A support and update tracking system.
- Description and sample of what a 'Statement of Compliance' is.

3. What is the PSTI Act and its Regulation

Manufacturer's compliance to the minimum-security requirements on hardware and software is based on the UK's Code of Practice for Consumer IoT security.

The leading global standard for consumer IoT security is ETSI EN 303 645 set against 13 controls. Currently, only three are required in sections 5.1, 5.2 & 5.3 of the standard (pages 13, 14, & 15) on condition that the manufacturer complies with provision 'Schedule 2' of the Act and on advice from the UK's technical authority for cyber threats, the National Cyber Security Centre (NCSC).

IT Security techniques – Manufacturer vulnerability disclosure 'Schedule 2' of the Act can be implemented by ETSI EN 303 645 on prevision 5.2-1 and / or BS EN ISO/IEC 29147:2020, on paragraphs 6.2.2, 6.2.5, and 6.5 of the standard on reporting security issues.

The OPSS regulatory authority will also ensure other businesses in the supply chains of manufacturers, importers and distributors of these products play their role in preventing insecure consumer products from being sold to UK consumers and businesses.

4. Basic idea and purpose of the Act

By setting legal standards and requirements for the security of these devices, the Act aims to protect consumers from the potential cyber threats that exploit vulnerabilities in poorly secured devices.
The three control provisions overview on compliance with the Act from the ETSI EN 303 645 Standard would include:

- **5.1 Unauthorised access** – No weak passwords, i.e. No Default Passwords! – All IOT-based products would require secure, unique passwords or those defined by the user. i.e., They must not be based on incremental counters; based on or derived from publicly available information; based on or derived from unique product identifiers, such as a serial number unless this is done using an encryption method, or keyed hashing algorithm, which is accepted as part of good industry practice; or otherwise easily guessable.

- **5.2 Implement a means to manage disclosure of vulnerabilities** – A Coordinated Vulnerability Disclosure (CVD) program in place. Requiring manufacturers to publish contact information to allow vulnerabilities relating to their products to be reported.

- **5.3 Keeping software up to date** – Mandate that manufacturers provide transparency on for how long, at a minimum, the product will receive security updates. And a support period defined in your policy. To mitigate from forms of cyber attacks that exploit vulnerabilities in insecure devices. For example, vulnerabilities in firmware, or software App or internet web-based software by infrastructure inter-connected to the IOT hardware device. And the requirement of developing and deploying security updates in a timely manner.

5. Penalties for non-compliance of the Act

The penalties for non-compliance with the PSTI Act are quite stringent. Below are the key details:

- The maximum fine that can be imposed for non-compliance is £10 million, or 4% of the company's worldwide turnover, whichever is greater.

- Additional daily penalties in cases where non-compliance continues, there is a provision of a daily penalty, which can be up to £20,000 per day for not adhering to the Act's requirements.

The range of penalties besides financial can also include:

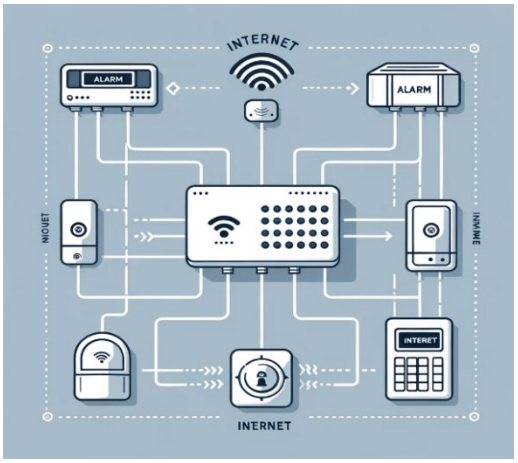
- **Stop Notices** – The supply chain selling the device would need to stop selling it until it's fully compliant.

- **Recall Notices** – The full recall of a noncompliant devices.

- Liability for directors/partners and other responsible persons within a company being held accountable.

6. Examples of alarm systems that are in scope and not in scope of the PSTI Act

No device is connected to a LAN, WAN, or the internet. However, wireless devices connected to the alarm panel in the picture above are not connected to the internet. Firmware updates are allowed via the USB port on the alarm panel if it or any of its devices do not connect to a LAN, WAN, or the internet. In this case, it is not in the scope of the PSTI Act.



It is in the Scope of the Act as the alarm panel is connected to a LAN or WAN wireless network or the internet. Although there are wireless devices connected to the alarm panel.

7. Manufacture, Distributor and Importer Definitions

Section 7: Relevant persons (taken from Commentary on Provisions of Act)

This Section defines the economic factors to which the duties set out in Part 1 apply. "Relevant persons" are defined as manufacturers, importers and distributors of relevant connectable products.

51. Subsection (3) defines "**manufacturer**" as a person who (i) manufactures a product, or has a product designed or manufactured, and (ii) markets that product under their own name or trademark. A person who markets under their own name or trademark a product manufactured by another person is also a manufacturer.

52. Subsection (4) defines "**importer**" as a person who (a) imports the product into the United Kingdom from another country, and (b) is **not** a **manufacturer** of the product.

53. Subsection (5) defines "**distributor**" as any person who (a) makes the product available in the United Kingdom, and (b) is **not** a **manufacturer** or an **importer** of the product.

54. Subsection (6) provides that a person will "**not**" be considered a **distributor** if they make the product available by performing a contract consisting of or including the installation of the product in a building or structure. This only applies if products identical to the installed product are or have been made available to consumers outside of such a contract for their installation. (This basically makes the normal UK Security Installers exempt from being a Distributor)

    Example provided to define a Distributor (As long as they are **not** a **Manufacturer,** or an **Importer** see 54 above)

    "A family hires a company "A" to install a bespoke smart security system in their home. The family pays for the entire project (including design, production, installation and the products). The products that form the smart security system can only be purchased from company A as part of a contract that involves their installation. The products are unique and are not made available to consumers in any other way. Company A is a distributor of the products."

    In other words, the Installer would only be classified as a Distributor, if the product is "exclusive" to them and can only be installed by them as part of the contract.

    In the UK security market, the same products can normally be purchased and installed by another installer, so the customer has a choice of who and what they use for their premises and therefore the installer is not classified as a Distributor.

8. Developing a Comprehensive Product Support and Update Tracking System

8.1. System Security and cyber related threats

Security systems benefit from network connectivity for enhanced functionality. However, this connectivity also exposes them to a range of cybersecurity vulnerabilities. The Common Vulnerabilities and Exposures (CVE) (http://cve.mitre.org) system, a widely recognised list of publicly disclosed cybersecurity vulnerabilities and exposures, highlights several potential security issues that can affect these systems, such as:

- **Insecure Default Settings**: Devices set up with default passwords are particularly vulnerable to unauthorized access. This is a common issue with many connected security devices where default settings may not prioritise security.
- **Buffer Overflows**: This occurs when a device receives more input data than it can process, potentially allowing an attacker to execute malicious code, affecting the integrity of security systems.
- **Injection Flaws**: Security systems with web interfaces or network connectivity might be susceptible to injection attacks, such as SQL (Structured Query Language), NoSQL, OS (Operating System), and LDAP (Lightweight Directory Access Protocol) injection, compromising data integrity and confidentiality.
- **Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF)**: These vulnerabilities can affect the web interfaces of security devices, leading to unauthorised commands or data breaches.

- **Inadequate Encryption**: The absence or weakness in encryption mechanisms can make data transmission vulnerable to interception, a significant concern for devices transmitting sensitive security data.
- **Firmware Update Issues**: Lack of secure firmware update mechanisms can leave devices with unpatched vulnerabilities, making them susceptible to exploits based on known issues.
- **Physical Security Weaknesses**: The hardware components of these systems may be vulnerable to tampering, which could compromise device functionality and security.

In addition to the CVE, several other systems and frameworks help identify and manage vulnerabilities:

- **Common Vulnerability Scoring System (CVSS)**: This system provides a standardised way to score vulnerabilities' severity, helping prioritise responses to security threats.
- **Common Weakness Enumeration (CWE)**: This categorises common software weaknesses and vulnerabilities, offering insight into potential security issues that could lead to vulnerabilities.
- **National Vulnerability Database (NVD)**: This U.S. government repository provides a comprehensive database of vulnerability management data, including descriptions and severity scores.
- **Open Web Application Security Project (OWASP)**: Although more focused on web applications, OWASP's guidance on security risks is relevant for network-connected security devices.
- **Vendor-Specific Databases**: Manufacturers may also maintain databases of vulnerabilities specific to their products, providing patches and updates for known issues.

Awareness and proactive management of these vulnerabilities are essential for developers, manufacturers, and users of security systems. Implementing best practices for security such as regularly updating device firmware, changing default settings, employing strong encryption, and monitoring unusual activities can significantly mitigate the risk of cyberattacks and ensure the integrity of security infrastructures.

8.2. Developing a Comprehensive Product Support and Update Tracking System

A comprehensive spreadsheet or database is crucial to effectively track and manage product support periods, especially in compliance with regulations like the PSTI Act that mandates products to have defined support durations for application and firmware updates (including CVE security updates).

Here is a suggested list of column headings for the product tracking spreadsheet, database:

- **Make -** The manufacturer of the product.
- **Model -** The specific model of the product.
- **Model Number -** The unique identifier for the specific version of the model.
- **Product Category -** Product type (e.g., software, hardware, IoT device).
- **Batch Number:** Product batch number.
- **Release Date -** The date when the product was first released.
- **End of Life Date -** The manufacturer's officially announced date when the product will no longer receive support or updates.
- **Support Period Start Date -** The date when the support for the current version of the application or firmware begins. – A PSTI Act requirement.
- **Support Period End Date -** The date when the support for the current version of the application or firmware is scheduled to end. – A PSTI Act requirement.
- **Application Update Support -** Indicating whether application updates are supported (Yes/No).
- **Firmware Update Support -** Indicating whether firmware updates are supported (Yes/No).
- **CVE Security Updates Support -** Indicating whether CVE security updates are specifically supported (Yes/No).
- **CVE-ID -** Vulnerability Identification code - http://cve.mitre.org.

- **CVE Description –** Description of publicly discovered vulnerability - http://cve.mitre.org.
- **Last CVE Security Update -** The date of the last CVE security update, if applicable.
- **Vulnerability Non-disclosed ID -** Vulnerability ID code for security issue/s not covered by a publicly disclosed CVE.
- **Vulnerability Non-disclosed Description -** Description of the vulnerability of either the application or firmware of the device.
- **Vulnerability Non-disclosed Date -** Vulnerability of security issue/s first discovered date.
- **Last Non-disclosed Vulnerability Update -** The last date of the non-disclosed vulnerability update patch with the associated 'Vulnerability Non-disclosed ID' code.
- **Security Update Frequency -** Expected frequency of update/s (e.g., monthly, quarterly, as needed).
- **Last Application Update -** The date of the last application update.
- **Last Firmware Update -** The date of the previous firmware update.
- **Update Frequency -** Expected frequency of updates (e.g., monthly, quarterly, as needed).
- **Contact Information for Support -** Contact details for product support (could be a URL, email, or phone number).
- **Documentation Link -** A direct link to the product support and update documentation. i.e., user manual (hardware/software), installation manual, changing the device's default password, etc.
- **Notes -** Any additional notes or comments about the product's support, updates, or other relevant information.

This is a basic list that aims to cover the essential aspects of tracking support and update periods for products under the PSTI Act or similar regulations. Depending on your specific requirements or the nature of the products being tracked, it might need adjustment or extending this list with additional columns.

8.3. Support Website Suggestions

Suggested spreadsheet column headings can be included in a website, particularly in a dedicated section for product support and updates or in a comprehensive product database. Here is how this information could be structured and utilized on a website:

Product Support Section

- **Web Pages for Each Product:** Create individual pages for each product in your database. These pages can include all the details from the spreadsheet/database, such as make, model, model number, support periods, and update information etc.
- **Searchable Database:** Implement a searchable database feature that allows users to search for products by make, model, or model number. This database would display relevant information, including support periods, update support status, and last update dates.
- **FAQs and Support Documentation:** Link to FAQs and support documentation for each product, providing users with easy access to detailed information about support policies, how to update their products, and how to address common issues.
- **Update Logs:** Maintain a log or bulletin for each product where updates (application updates, firmware updates, and CVE security updates) are chronologically listed, along with their release notes and installation instructions.
- **Support Contact Information:** Offer a section with contact information or a support ticket system for users to reach out with specific questions or issues regarding their products.

Technical Considerations for Website Integration

- **User Interface Design:** Ensure the website is designed with user experience in mind, making it easy for visitors to navigate through product information, find support details and access update logs.
- **Database Management:** Implement a robust backend database system to efficiently store, manage, and retrieve detailed product information. This system should support real-time updates to ensure the information presented on the website is current.

- **Security and Privacy:** Secure the website and database to protect sensitive information and ensure compliance with relevant data protection regulations. It includes securing user inquiries and any personal data submitted through the website.
- **Accessibility:** Ensure the website is accessible to users with disabilities, adhering to web accessibility standards to ensure all users can find and understand the product support information.

By incorporating this data into a website, companies can offer transparent, accessible support and updated information to their customers, thereby enhancing customer service and compliance with relevant regulations like the PSTI Act.

8.4. Addressing non-disclosure vulnerabilities

Handling non-disclosed vulnerabilities in product support and updates, in line with PSTI Act requirements, demands careful tracking and communication strategies. Here is how to incorporate this into the aforementioned spreadsheet/database and website.

In the Spreadsheet / Database:

Adding columns related to non-disclosed vulnerabilities can help in internal tracking and risk management.

Consider these additional headings:

- **Non-Disclosed Vulnerabilities Identified** - A Boolean or status field indicating whether non-disclosed vulnerabilities have been identified for the product.
- **Risk Assessment of Non-Disclosed Vulnerabilities** - A summary field indicating the potential impact or risk level of identified non-disclosed vulnerabilities.
- **Mitigation Plan for Non-Disclosed Vulnerabilities** - A brief description of the planned or implemented mitigation strategies for these vulnerabilities.
- **Mitigation Status** - Current status of the mitigation efforts (e.g., In Progress, Completed).
- **Internal Notes on Non-Disclosed Vulnerabilities** - Any additional internal notes regarding the non-disclosed vulnerabilities, including potential disclosure plans or coordination with security researchers.

On the Website:

While non-disclosed vulnerabilities present a challenge in public communication, transparency about handling such vulnerabilities can build trust. Here is how to approach it:

- **Security Policy and Vulnerability Management Page**: Create a page detailing your company's approach to security, including how vulnerabilities are handled, without disclosing sensitive details. Emphasise commitment to security, the process for investigating potential vulnerabilities and how updates are provided to address them.
- **Responsible Disclosure Program**: If applicable, detail your responsible disclosure program, encouraging ethical hackers or researchers to report vulnerabilities securely. It shows a proactive stance on security without revealing specific vulnerabilities.
- **Update Notifications**: Without specifying non-disclosed vulnerabilities, regularly update customers on security improvements and patches. It could be part of a broader update log or bulletin mentioned earlier.
- **Customer Assurance Statements**: Include statements assuring customers that security is a top priority and that all known publicly disclosed vulnerabilities are being addressed through updates and patches by best security practices.

Communication and Policy:

- **Internal vs. External Communication**: Maintain clear guidelines on what information is communicated internally versus publicly disclosed. It helps manage the information flow regarding non-disclosed vulnerabilities while ensuring that internal stakeholders are informed and prepared.
- **Compliance and Legal Considerations**: Ensure that the approach to handling non-disclosed vulnerabilities complies with relevant laws and regulations, including any obligations to report or disclose vulnerabilities under specific circumstances.

By integrating these considerations into the tracking system (spreadsheet/database) and public-facing information (website), organisations can manage non-disclosed vulnerabilities effectively while maintaining transparency and trust with their users.

9. Statement of Compliance requirement PSTI Act 2022

9.1. Content of the Statement of Compliance

The Statement of Compliance in relation to the PSTI Act regulation is a crucial document that manufacturers of relevant connectable products must prepare and retain to make their products available in the United Kingdom. This document serves as evidence that the manufacturer has met the specific regulatory requirements related to the security and compliance of their products against reference to Schedule 4 - **2023 No. 1007 CONSUMER PROTECTION -** The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023. The key components and requirements of the Statement of Compliance can be summarised as follows:

- **Product Details**: Information about the product type and batch.
- **Manufacturer and Representative Details**: Names and addresses of the product's manufacturers and, if applicable, their authorised representatives.
- **Declarations by Manufacturer**: Two declarations are required:
  - A declaration confirming the statement is prepared by or on behalf of the manufacturer.
  - A declaration stating the manufacturer's belief in their compliance with the applicable security requirements outlined in Schedule 1, or the deemed compliance conditions in Schedule 2 of the regulation.
- **Support Period**: The defined support period for the product, accurate at the time of the product's first supply.
- **Signatory Details**: Signature, name, and function of the person signing the statement, along with the place and date of its issue.

Compliance with Standards - If compliance involves conformity to a specific standard (as referenced in sub-paragraph ((1)(d)(ii)), the statement must include the identification number, version, and date of issue of the standard.

Minimum Information Requirement – Schedule 4 of the regulation outlines the minimum information that must be included in the statement.

Manufacturer's Retention of the Statement:

- The manufacturer is required to retain a copy of the statement for the longer of:
  - 10 years from the date of issue.
  - The defined support period for the product, as stated in the statement.

Legal Requirement for Availability in the UK

A manufacturer must not make a relevant connectable product available in the UK unless it is accompanied by a Statement of Compliance or a summary of it, as specified by regulations made by the Secretary of State.

Regulatory Oversight

- The Statement of Compliance must affirm the manufacturer's opinion of compliance with the applicable security requirements, excluding those that apply post-release in the UK or specifically to UK customers.
- Provisions for joint manufacturers, further regulatory definitions, retention requirements, publishing, and distribution of the statements are outlined, with specific conditions and regulations subject to affirmative or negative resolution procedures.

This framework ensures that manufacturers are accountable for the security and compliance of their connectable products, safeguarding consumers and aligning with the UK's regulatory standards.

Note: Please refer to section 9 for an example of the 'Statement of Compliance'.

10. Statement of Compliance draft example under

Schedule 4 of the PSTI Act

10.1. 'Statement of Compliance' example

Statement of Compliance example below - Reference to Schedule 4 - **2023 No. 1007 CONSUMER PROTECTION -** The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023'.

Statement of Compliance

Product Details:

- **Type: {including Make, Model, Model Number}**
- **Batch Number**: **{Production batch number}**

Manufacturer Information:

- **Name: {Company name}**
- **Address**: **{company address details}**
- **Authorised Representative** (where applicable): **{Representative name if applicable else Not Applicable}**

Declaration of Compliance:

1. **On Behalf of the Manufacturer**: I hereby declare that this statement of compliance is prepared by or on behalf of {company name}., the manufacturer of the **{including Make, Model, Model Number}.**

   - **Compliance with Schedule 1**: **{Company name}.** Hereby declares that the **{including Make, Model, Model Number}** meets the direct security requirements as specified in **Schedule 1** of the regulation. To explicitly demonstrate this compliance, our product adheres to the **{standard ID number and description i.e. ISO/IEC BS EN xxxxx}**, in adherence with ETSI EN 303 645 v.2.1.1, 19th June 2020 which aligns with the principles outlined in Schedule 1, particularly in terms of secure development lifecycle, system integrity, data confidentiality, and user authentication. This standard ensures that our product's security measures are robust, comprehensive, and directly compliant with the required security principles.

     Standard Details:

     - **Standard**: **{IEC ISO number including year}**
     - **Compliance Date**: **{Date, Month, Year}**

   - **Compliance with Schedule 2**: In addition to our direct compliance with the security requirements of Schedule 1 through adherence to {**standard ID number and description i.e. ISO/IEC BS EN xxxxx**}, the Smart Home Security Camera has also achieved certification under the **{related Cyber Security Standard certification}** in adherence with ETSI EN 303 645 v.2.1.1, 19th June 2020 which aligns with the principles outlined in **Schedule 2** for providing equivalent or superior security assurance. This dual approach underscores our commitment to ensuring the highest security standards for our products and provides an additional layer of confidence in our compliance and security measures.

     Certification Details:

     - **Certification Program**: **{Certification program i.e. Global IoT Security Standard / Pen test}**
     - **Certification ID** : **{Certification identification Number}**
     - **Date of Certification**: **{Date, Month, Year}**

Support Period:

- The defined support period for the **{Product, Make, Model description}** is **{number}** **years** from the date of first supply, during which **{Company name}.** commits to providing necessary security updates and technical support.

Signatory Details:

- **Signature**: **{Digital Signature of Authorized Individual}**
- **Name**: **{Individual's name}**
- **Position: {Position in company}**
- **Place of Issue**: **{Area, Country}**

Date of Issue: **{Date, Month, Year}**

Note: Highlighted blue text within the curly brackets {..} are examples to be replaced with actual manufacturer text i.e. product make, model descriptions etc. The above hypothetical 'Statement Of Compliance' example is for illustrative purposes only.

10.2. Schedule 4 clause 1. d. - Applicable security requirements in Schedule 1 or the deemed

compliance conditions in Schedule 2.

The previous example, 'Statement of Compliance' on page 9, could reference either Schedule 1 and Schedule 2 or both, particularly when a product meets direct security requirements and holds certifications or adheres to standards deemed equivalent or supplementary to those requirements. Incorporating both schedules might enhance the product's compliance profile, demonstrating adherence to specific regulatory mandates and a commitment to broader security principles and practices recognised within the industry. This approach can prove a manufacturer's dedication to security, potentially exceeding the minimum regulatory requirements.

Disclaimer:
This example '**Statement of Compliance'** is provided for illustrative and guidance purposes only. It is intended to serve as a general template that outlines the potential structure and content required for compliance with the relevant regulatory standards and requirements. The information provided herein does not constitute legal advice, nor is it intended to cover all possible legal obligations, requirements, or implications related to creating, submitting, or maintaining a Statement of Compliance. Regulatory requirements are subject to change, and the applicability of specific standards or compliance measures can vary widely depending on the product, its use cases, and the location in which it is marketed and sold. Therefore, it is critically important that manufacturers or responsible parties consult with a qualified legal professional or a compliance expert to review and tailor this document to meet the specific legal and regulatory requirements applicable to their product. This review should ensure that the Statement of Compliance accurately reflects the product's compliance status and adheres to current legal standards and best practices. Reliance on this example without conducting a thorough legal and compliance review may result in inaccuracies, non-compliance, or other legal challenges. The BSIA, the creators of this example, and any affiliated parties disclaim any liability for actions taken or not taken based on the content of this example.

References

The UK Product Security and Telecommunications Infrastructure (Product Security)
https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime

PSTI Regulation - Commentary on provisions of Act
https://www.legislation.gov.uk/ukpga/2022/46/notes/division/6/index.htm

OPSS – Office for Product & Standards (Regulatory Authority)
https://www.gov.uk/government/organisations/office-for-product-safety-and-standards

Guidance - Code of Practice for Consumer IoT Security
https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

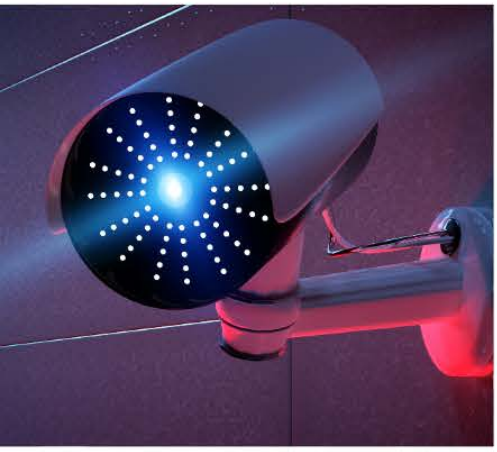
The National Cyber Security Centre (NCSC) - https://www.ncsc.gov.uk/

ETSI - Consumer IoT security - https://www.etsi.org/technologies/consumer-iot-security

ETSI - EN 303 645 - V2.1.1 (2020-06) - CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirement
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Mitre Organisation - https://cve.mitre.org/

OWASP Foundation - https://owasp.org/contact/



About **the BSIA**

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security. For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.