BCS’ Response to the Department for Science, Innovation and Technology’s Call for Views on Enterprise Connected Device Security

July 2025

Table of Contents

BCS
The Chartered Institute for IT
3 Newbridge House,
Newbridge Square,
Swindon SN1 1BY
BCS is a registered charity: No 292786

1 Executive Summary

Summary of BCS, The Chartered Institute for IT, response to the Government's Call for Views on Enterprise Connected Device Security

BCS broadly welcomes the UK Government's proposals to enhance the security of enterprise connected devices and supports the development of a dedicated Code of Practice (CoP) to ensure best cyber security practices are adopted across enterprise technologies.

1.1.1 Support for Key Security Principles

BCS *strongly agrees* with the inclusion of most of the 11 proposed principles for the Code of Practice, which aim to improve device security through areas such as secure software updates, authentication, encryption, integrity, logging, and recovery capabilities. Specific BCS feedback includes:

- **Secure Updates (Principle 1):** Supported in full. BCS recommends ensuring administrators can manage updates across device estates and that update policies clearly address known vulnerabilities.
- **Authentication (Principle 2):** Strongly supported. BCS urges clearer guidance to ensure pre-installed credentials are randomised and not derived from predictable device identifiers.
- **Data Protection (Principle 3):** Strongly supported. BCS suggests referencing NCSC cryptographic best practices and encourages more specificity around data compartmentalisation.
- **Device Integrity (Principle 4):** Fully endorsed, with suggestions to clarify that update mechanisms should be *secure*, and terms like "boot integrity" should be explicitly stated.
- **Device Health Monitoring (Principle 5):** BCS **disagrees** with its inclusion as a standalone principle, suggesting it lacks clarity and measurable objectives.
- **Trusted Software (Principle 6):** BCS neither agrees nor disagrees. Concerns were raised over the practicality of implementing trust-based access control across all user scenarios.
- **Application Privilege (Principle 7):** Strong support, with encouragement for granular permission models and strict software compartmentalisation.
- **Device Interfaces (Principle 8):** Strong support. BCS recommends switching the order of some guidelines for improved logical flow.
- **Device Management (Principle 9):** Strong support. Suggests local configuration should only be allowed at first use; thereafter, all changes should go through device management services.
- **Logging and Monitoring (Principle 10):** Fully supported. BCS recognises the importance of enabling accurate and secure audit trails.
- **Device Recovery (Principle 11):** Strong support, with a recommendation to strengthen guideline 11.4 by explicitly requiring *immutable backups*.

1.1.2 Broader Policy Recommendations

BCS agrees that:

- There is a need for government action to **encourage greater cyber security** in enterprise devices, but it should focus on enabling manufacturers to support enterprise compliance with existing sectoral regulations.
- **Enterprise connected devices differ sufficiently** from consumer IoT to warrant a **separate Code of Practice**, rather than expanding the existing Product Security and Telecommunications Infrastructure (PSTI) Act 2022.

1.1.3 On Implementation and Practical Challenges

BCS, speaking as an industry body, acknowledges that while many principles are desirable, there may be **practical implementation challenges** for some organisations depending on size, resources, and device complexity.

1.1.4 Preferred Policy Interventions

BCS ranks proposed government interventions as follows:

1. **Creating a new global standard**.
2. **Creating a voluntary pledge**
3. **Introducing new legislation that creates legal obligations for enterprise connected device manufacturers**
4. **Broadening the scope of the consumer IoT legislation (PSTI Act 2022)**

1.1.5 Conclusion

BCS supports a **clear, standalone Code of Practice** for enterprise connected devices, underpinned by **global standards and voluntary commitments**, and backed by **targeted legislation where appropriate**. The aim should be to **empower manufacturers** to build secure devices and support enterprises in meeting their broader regulatory obligations.

Who we are

BCS is the UK’s Chartered Institute for Information Technology. The purpose of BCS as defined by its Royal Charter is to promote and advance the education and practice of computing for the benefit of the public.

We bring together industry, academics, practitioners, and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for Information Technology we serve over 60,000 members including practitioners, businesses, academics, and students, in the UK and internationally.

We also accredit the computing degree courses in over ninety universities around the UK. As a leading information technology qualification body, we offer a range of widely recognised professional and end-user qualifications.