Research and Analysis Exploring the ‘Enterprise Internet of Things (EIoT)’

A report produced by Copper Horse Ltd.

March 2025

Executive summary

This work set out to test a definition of Enterprise IoT (EIoT) defined by the National Cyber Security Centre (NCSC) as well as to conduct a desk-based review of published material to discover the current status of views towards IoT in the Enterprise and any existing definitions. The work explores material from across the world from companies to standards bodies.

The paper also summarises a series of interviews that were conducted with experts from across the IoT domain. The semi-structured interviews sought to understand the interviewees' opinions on Enterprise IoT and to test the NCSC definition of EIoT.

The report concludes that developing a single, universal definition of EIoT is neither feasible nor advisable. The evidence suggests that rigid categorisations risk oversimplifying a complex technological and cyber security risk landscape. Existing definitions of IoT are already fragmented, for example with differences between countries considering laptops and mobile devices as in the scope of IoT or not. These basic differences and the complexity of IoT deployments may hamper efforts to develop clear, proportionate and effective government policy. It may lead to a decrease in cyber security as companies seek to avoid measures designed to improve IoT security when deployed in the Enterprise.

The researchers propose a more flexible, context-driven approach that reflects the diversity of IoT deployments horizontally across different sectors and use cases. The adoption of core baseline security measures across the entirety of IoT, combined with classification of devices and solutions themselves based on their real-world usage, may be a more effective approach than artificially creating requirements by the office/enterprise element inside business sectors.

Introduction

This report presents the findings of a research study commissioned and funded by the UK Government's Department for Science, Innovation and Technology (DSIT) undertaken to support future work of the Critical Technologies Policy Team. The aim of this research is to review existing definitions and framings of Enterprise IoT and build on the National Cyber Security Centre's (NCSC) definition to develop an updated, practical definition that can be used to inform DSIT's future policy approach and support market research.

This study was conducted between February and March 2025 and draws on extensive desk research along with expert interviews to examine current interpretations of EIoT.

Supporting materials, including references and interview details are provided in the appendices.

Scope and Methodology

Approach

This report combines desk research and expert interviews to develop a comprehensive definition of Enterprise Internet of Things (EIoT).

Copper Horse researchers reviewed existing definitions and frameworks from national and international organisations, such as the UK's National Cyber Security Centre (NCSC), Ofcom, US Federal Communications Commission (FCC) and the European Union Agency for Cybersecurity (ENISA). The team also looked at definitions from industry organisations including Microsoft, Amazon Web Services (AWS) and the IoT Security Foundation (IoTSF), alongside relevant academic research to understand prevailing views on EIoT.

In the desk research, the researchers analysed market trends, technological developments and the regulatory landscape affecting EIoT. They reviewed reports from government agencies, IoT vendors and industry publications.

The researchers conducted interviews with industry professionals, cyber security analysts and academics to test existing definitions and gather different views on EIoT. See the Interview Process section below for more details and the Appendices for further information on the breakdown of interviewees and the questions.

This approach ensured the report was grounded in both theoretical and practical insights, enabling a comprehensive definition that reflects real-world applications and challenges.

Interview Process

To ensure a diverse and representative set of insights, the researchers selected interviewees based on the following experience:

- industry expertise: professionals working in IoT security, telecommunications, enterprise information technology (IT) and regulatory compliance

- academic inputs: researchers in cyber security, AI and IoT with a focus on enterprise applications
- regulatory and policy experience: experts involved in developing and implementing government mandated IoT security standards and policies
- market practitioners: representatives from technology companies that manufacture, deploy, or manage EIoT solutions

Copper Horse conducted interviews using a semi-structured approach. This allowed participants to discuss pre-selected topics and raise new concerns not covered in existing research. Key areas explored included:

- definitions and classifications of EIoT
- distinctions between EIoT, consumer IoT and Industrial IoT (IIoT)
- the role of enterprise-scale deployment and device management in defining EIoT
- the role of cyber security, privacy and regulation defining EIoT
- perspectives on existing definitions such as from the NCSC
- future considerations and potential improvements to the definition

Scope Limitations

While this research provides a broad and well-informed perspective on EIoT, certain scope constraints must be acknowledged:

- this report does not cover Operational Technology (OT) or sector-specific IoT applications in highly regulated industries such as healthcare and automotive
- this report is accurate as of March 2025, as the IoT landscape is rapidly evolving and definitions may require updates as technology and market trends shift
- while the researchers have incorporated a range of viewpoints, individual biases and organisational perspectives may influence responses
- the limited time and budget of the project kept the participant numbers to a small number

Despite these scope limitations, this report provides a well-rounded foundation for policymakers and industry stakeholders to understand a range of views and definitions that include EIoT.

Existing Definitions

Definitions of EIoT

This first section focuses on definitions that explicitly mention IoT in the context of the enterprise. Once these are established, the next section broadens the scope to include general IoT definitions that mention enterprise applications. This approach ensures that the discussion remains grounded in enterprise-specific terminology before exploring how EIoT fits in with the wider, more commonly defined IoT landscape.

Definitions of EIoT previously used by some UK public bodies

The National Cyber Security Centre (NCSC) – The UK's technical authority for cyber threats defines EIoT in this article as:

> *"Enterprise IoT is the advancement in technology that enables physical 'things' with embedded computing devices to participate in business processes for reducing manual work and increasing overall business efficiency. Taking advantage of a combination of technologies ranging from embedded devices with sensors and actuators to internet-based communication and cloud platforms, enterprise IoT applications can now automate business processes that depend on contextual information provided by programmed devices such as machines, vehicles, and other equipment."*
>
> ***NCSC – Organisational use of Enterprise Connected Devices (2022)***
>
> *[NCSC 2022]*

This definition highlights how EIoT extends beyond traditional automation by incorporating cloud platforms and internet communication into physical infrastructure, allowing businesses to streamline operations and improve decision-making. Unlike consumer IoT, which is designed for personal use, EIoT operates at a larger scale, integrating with business-critical systems.

The NCSC further clarifies that EIoT devices are "industry-agnostic and are typically not available or intended for consumers to purchase" and are distinct from traditional Operational Technology (OT) systems, which focus on industrial control processes rather than networked automation.

The UK Parliament Committee Report on Connected Tech provides contextual clarity on EIoT, stating in this report that:

> *"Connected tech used by businesses and organisations, such as in offices, healthcare and transport, are sometimes referred to as*

> *'enterprise IoT' technology (EIOT); connected tech used in industrial settings, like manufacturing, agriculture and energy infrastructure, are often referred to as 'industrial IoT' (IIoT)"*
> ***UK Parliament – Connected tech: smart or sinister? (2023)*** *[UK Parliament 2023]*

This distinction reinforces the idea that EIoT encompasses connected technologies used within general business, office and public service environments, separate from IIoT, which is focussed on large-scale, sector-specific automation.

By framing EIoT as a distinct category within connected technology, the report highlights its widespread presence in commercial and organisational settings, where devices such as smart office systems, healthcare monitoring tools and connected transport infrastructure play an increasingly significant role. This classification is significant in discussions on IoT security, policy and regulation, as enterprise environments often operate under different cyber security requirements than industrial systems. The UK Parliament's inquiry into connected technology underscores the need for targeted security measures and governance frameworks to address the unique challenges associated with EIoT, recommending these devices are safeguarded within business and public sector applications.

Industry and Organisational Definitions of EIoT

Microsoft explicitly classifies EIoT by the types of devices involved:

> *"eIoT includes printers, scanners, cameras, Smart TVs, VoIP phones, and other purpose-built devices used to streamline enterprise processes."*
> ***Microsoft – Defender for IoT (2022)*** *[Microsoft 2022]*

This categorisation highlights the role of connected devices in enhancing workplace efficiency, where smart office technology integrates seamlessly with traditional IT infrastructure to support business operations. EIoT is deployed in corporate environments to optimise workflows, improve communication and enhance automation across industries.

Microsoft's approach underscores the importance of securing and managing EIoT devices alongside traditional IT assets. As these devices become more deeply embedded within business networks, they introduce new cyber security risks, requiring advanced threat detection, network monitoring and access controls.

IoT cloud services provider AWS defines the Internet of Things broadly as:

> *“IoT, or Internet of Things, refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves ... Industrial IoT (IIoT) refers to smart devices used in manufacturing, retail, health, and other enterprises to create business efficiencies. Industrial devices, from sensors to equipment, give business owners detailed, real-time data that can be used to improve business processes. They provide insights on supply chain management, logistics, human resource, and production – decreasing costs and increasing revenue streams.”*
> ***AWS – What is IoT? (2024)*** *[AWS 2024]*

This definition encompasses a wide range of applications, including enterprise environments, where AWS acknowledges that a “whole industry has sprung up” around integrating IoT devices into “homes, businesses and offices.” The inclusion of business settings highlights the role of EIoT in transforming workplace operations, leveraging connectivity to enhance efficiency, streamline workflows and support data-driven decision-making.

AWS explicitly mentions enterprise under the term IIoT. This definition blurs the lines between EIoT and IIoT by positioning both as a part of the same business optimisation strategy. While IIoT traditionally focuses on manufacturing and industrial automation, AWS’ definition suggests that the nature of their deployments is not too dissimilar to one another. This convergence indicates the distinction between enterprise and industrial may not be so significant, since they both rely on connected devices, real-time analytics and automation to improve business operations across various sectors.

TechUK has provided views on IoT security. While TechUK does not publish a formal definition, it echoes government descriptions. For example, following a 2022 engagement with the Department for Digital, Culture, Media & Sport (DCMS), (the department formerly responsible for this policy domain), TechUK recorded that DCMS had been conducting a review into:

> *“enterprise IoT or enterprise connected devices, such as office printers, office cameras and room booking systems.”*
> ***DCMS/techUK Roundtable – Enterprise IoT and Connected Device Security (2022)***

This definition reflects an understanding that EIoT encompasses a broad category of non-consumer, networked devices deployed in business settings to support operations and efficiency.

By reinforcing this perspective, techUK underscored the significance of EIoT in workplace environments, where connected devices play an essential role in modern business infrastructure. The inclusion of printers, cameras and office management systems highlights the everyday nature of EIoT, distinguishing it from IIoT while emphasising the need for robust security measures. As businesses continue integrating connected technologies, techUK's engagement with the UK government highlights the importance of securing EIoT devices against cyber threats, ensuring they remain a reliable part of organisational operations. [TechUK 2022]

The IoT Security Foundation (IoTSF) is a UK-based industry-led body that focuses on securing IoT. IoTSF's publications treat EIoT as the IoT ecosystem managed within an organisation. In their document titled 'IoT Security Architecture and Policy for the Enterprise' [IoTSF 2018] IoTSF states that enterprise solutions involve a wide range of connected assets owned/controlled by the enterprise and require frameworks for device onboarding, secure data handling and lifecycle management. IoTSF emphasises best practices to ensure that as businesses deploy IoT at scale, security and interoperability are maintained.

In their paper, the IoTSF emphasises the importance of a hub-based architecture for managing these devices securely. This approach involved a central hub that oversees the communication and security of connected devices, ensuring that they operate within the enterprise networks policies (and specifically on their own IoT network, as opposed to the standard business one). By implementing such an architecture, organisations can effectively monitor and control their IoT deployments, addressing challenges related to device authentication, network segmentation and data protection.

Academic Definitions of EIoT

Industry 4.0 is the phase of industrial change associated with digital systems becoming integrated into everyday business practices In .the academic paper titled 'Theory and Practice of Implementing a Successful EIoT Strategy in the Industry 4.0 Era' by Chehri and others [Chehri and others 2021], it specifies EIoT as a strategy within the context of Industry 4.0. The author defines IoT as:

> *"IoT technologies consist of objects to capture data: sensors, a network for transmission, data, information, and operating applications"*
>
> ***Chehri and others - Theory and Practice of Implementing a Successful Enterprise IoT Strategy in the Industry 4.0 Era (2021)***
>
> *[Chehri and others 2021]*

The paper highlights that EIoT enables businesses to connect, monitor and optimise operations by integrating sensors, actuators and cloud-based platforms to facilitate real-time data exchange. By leveraging Industry 4.0 technologies, enterprises can create smart factories where machines, products, suppliers and infrastructure collaborate seamlessly to enhance efficiency and competitiveness.

Beyond its role in connectivity and automation, the paper underscores the strategic challenges involved in designing and deploying EIoT solutions. Effective implementation requires robust network infrastructure, data interoperability and secure integration with Enterprise Resource Planning (ERP) and Manufacturing Execution Systems (MES). The authors note that EIoT is not just a technological advancement but a fundamental shift in industrial operations, requiring businesses to adopt new data governance models, cyber security frameworks and predictive analytics to ensure resilience and long-term sustainability in connected environments. [Chehri and others 2021]

In the academic paper titled 'Designing Enterprise Internet of Things Systems' [Gunadham 2024] EIoT is defined as:

> *"a group of technologies that enables internet-connected products and devices to send and receive data explicitly intended for enterprise applications"*
>
> ***Gunadham - Designing Enterprise Internet of Things Systems (2024)***
>
> *[Gunadham 2024]*

According to the paper, EIoT leverages IoT capabilities to identify, interact with and manage various enterprise elements such as "machines, products, collaborators, suppliers, customers and infrastructures". The primary goal is to create additional business value by optimising asset utilisation, enhancing operational efficiency, generating new revenue streams and improving product offerings.

Additionally, the paper identifies four critical components of EIoT systems: IoT Devices (sensors, wearables, actuators, etc), IoT Platform (software for device management and analytics), connectivity (the networks that facilitate data flow) and applications (enterprise software that utilises the data for operational insights). Together these components facilitate real-time monitoring and management of enterprise assets and activities.

IoTInsider notes that organisations use EIoT devices *"to increase productivity and enable hybrid working"*, implying the use of office machines, computers, printers, conference phones, etc but that these same devices introduce new cyber security challenges [IoTInsider 2022]. To combat these cyber security issues, the UK Government provided grants of up to £200,000 for researchers with the aim to understand how UK enterprises deploy and manage such IoT devices on their networks and to explore the risks that these devices present within businesses [IoTInsider 2022] [GOV.UK 2021]. Other research bodies such as PETRAS-IoT which aims to pair over 120 industrial and government partners with twenty-four research institutions to ensure that research can be "directly applied to benefit society, business and the economy". This highlights the importance that securely implemented IoT can bring to businesses. [PETRAS-IOT 2024]

International Definitions of EIoT

The United States' Federal Communications Commission (FCC), in establishing a national (voluntary) cyber security labelling program, explicitly distinguishes between consumer IoT and EIoT. According to the FCC's ruling:

> *"Consumer IoT Products vs. Enterprise IoT Products. The IoT Labeling Program applies to the labeling of consumer IoT products that are intended for consumer use, and does not include products that are primarily intended to be used in manufacturing, healthcare, industrial control, or other enterprise applications. While we do not foreclose expansion of the IoT Labeling Program at a later date, this initial scope will provide value to consumers most efficiently and expediently, without added complexity from the enterprise environment."*
> ***US Federal Register Vol. 89, No. 146 – FCC Cybersecurity Labeling for Internet of Things (2024)*** *[FCC 2024]*

This distinction reinforces that EIoT consists of devices designed for industrial, business, or organisational environments, separate from consumer-grade IoT products. While the labelling program currently focuses on consumer IoT, the FCC acknowledges the potential for future expansion to include EIoT, recognising the different security challenges posed by business and industrial deployments.

This approach is similar, but not directly comparable to the UK's Product Security and Telecommunications Infrastructure (PSTI) Act, which also prioritises consumer IoT security while leaving enterprise-focused requirements for a later stage. By excluding EIoT from its initial scope, the FCC's framework allows for a more immediate impact on consumer markets without the added complexity of enterprise security requirements. However, as businesses increasingly integrate IoT into critical operations, future policy developments will address EIoT cyber security, ensuring that organisations benefit from standardised protections and regulatory oversight.

Definitions of IoT with enterprise applications

The following section discusses definitions that make indirect reference to EIoT by mentioning IoT in general, or by combining enterprise, consumer and industrial IoT together. Their discussions are still important nonetheless to see where other countries stand in terms of definitions.

A definition used by Ofcom

Ofcom is the UK's statutory regulator for communications, also manages the use of the electromagnetic spectrum and defines IoT as:

> "IoT: Internet of Things. A system of connecting any electronic device to the internet and to other connected devices."
> ***Ofcom – Improving spectrum access for Wi-Fi (2020)*** *[Ofcom 2020]*

Ofcom adopts a broad definition of IoT in that article which applies across all aspects of IoT. While the report does not explicitly differentiate between consumer and EIoT, it does acknowledge enterprise use cases throughout, particularly in the context of spectrum demand and industrial applications. Ofcom highlights the growing reliance on IoT in manufacturing, logistics and smart infrastructure, noting that businesses are increasingly deploying wireless technologies, including Wi-Fi and private networks to enhance automation and efficiency. This aligns with the broader trend of enterprises integrating IoT for mission-critical operations that require low-latency and high-reliability connectivity.

By incorporating enterprise considerations into its spectrum planning, Ofcom signals the need to accommodate large-scale, business-driven deployments alongside consumer adoption. The report references "enterprise environments including stadiums, warehouse management and factory automation" [Ofcom 2020], which leverage wireless connectivity to improve flexibility and productivity, demonstrating Ofcom's recognition of IoT's role in industrial transformation.

International Definitions of IoT

The United States' IoT Cybersecurity Improvement Act of 2020 [US Congress 2020], which incorporates the US National Institute of Standards and Technology (NIST) guidance, defines IoT devices as those that:

> *"(A) have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional Information Technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and (B) can function on their own and are not only able to function when acting as a component of another device, such as a processor."*
> ***US Congress – IoT Cybersecurity Improvement Act of 2020*** *[US Congress 2020]*

This definition establishes IoT as distinct from traditional IT devices by focusing on physical-world interaction and network connectivity, ensuring that security measures account for the unique vulnerabilities of embedded, often unmanaged devices within enterprise and industrial environments.

A key aspect of this definition is its explicit exclusion of conventional IT devices such as smartphones and laptops, which are already well-defined within existing cyber security frameworks. Instead, the legislation applies to standalone IoT devices that can function independently, rather than being mere components of other systems. This scope reinforces the need for specialised cyber security approaches for IoT, acknowledging that traditional security models designed for computers and mobile devices may not be sufficient to protect IoT ecosystems, which often include sensors, smart appliances and industrial control systems that interact with critical infrastructure. Note that this differs to the UK's approach which has put these devices directly in-scope for consumer IoT in the Product Security and Telecommunications Infrastructure (PSTI) Act.

The United States' Cybersecurity & Infrastructure Security Agency (CISA) provides a broad definition of IoT, stating that it includes:

> *"any object or device that sends and receives data automatically through the Internet. This rapidly expanding set of "things" includes tags (also known as labels or chips that automatically track objects), sensors, and devices that interact with people and share information machine to machine."*
>
> ***CISA.GOV – Securing the Internet of Things (IoT) (2021) [CISA 2021]***

This description emphasises the data-sharing and automation capabilities of IoT but does not explicitly differentiate between consumer, enterprise, or industrial IoT. Instead, it presents a generalised view of IoT as a network of connected objects, covering a wide range of use cases from automated tracking and sensing to machine-to-machine communication.

While CISA's definition does not directly categorise EIoT separately, its reference to tags, sensors and machine-to-machine interactions aligns with technologies commonly found in enterprise and industrial environments. Businesses, logistics networks and smart infrastructure deployments rely heavily on these IoT components for asset tracking, operational monitoring and automated decision-making. However, without a clear distinction from consumer applications, CISA's framing suggests a broad security posture for all IoT devices rather than one specifically tailored to enterprise needs. Future policy discussions may further refine the security considerations for EIoT, where risks such as data integrity, network segmentation and large-scale device management present unique challenges beyond those faced in consumer applications.

The European Union Agency for Cyber Security (ENISA) study title 'Good Practices for Security of Internet of Things in the context of Smart Manufacturing', defines IIoT as:

> *"These devices have various capabilities, such as sensing, actuating, storing and/or processing information. What distinguishes them from traditional devices such as sensors and actuators that have been used in industrial applications for years is the fact that IIoT End Devices exchange data over the network. In Smart Manufacturing environments, by making large amounts of new types of data available, they contribute to streamlining production."*
>
> ***Good Practices for Security of Internet of Things in the context of Smart Manufacturing (2018) [ENISA 2018]***

This study defines IIoT devices as IoT technologies specifically applied within industrial settings, forming a critical subset of the broader industry 4.0 concept. Unlike traditional industrial equipment, IIoT devices actively exchange data across network, enabling machines to manage production autonomously in an efficient and resource-saving manner, leading to shorter production times and new services and business models.

The report also acknowledges several significant security challenges for businesses deploying IIoT, including managing vulnerabilities arising from interconnected devices, addressing security during IT and operational technology (OT) convergence and securing increasingly complex supply chains. The report makes note to separate IIoT devices into “Level 1” and Enterprise operations into “Level 4” discussing about their interoperability together, but their functions differing as Enterprise does not operate in real-time.

Germany’s Federal Office for Information Security (BSI) defines IoT as:

> *“connected world of smart devices. These IoT devices behave like computers and are connected to a local network or with other devices over the Internet. They are supposed to make our everyday lives easier, more comfortable and more efficient ... Wearables, smart home, smart toys, digital assistants and smart TVs are some examples of IoT devices and where they are used ... However, the terms Industry 4.0 and smart city are also closely related to the Internet of Things.”*
>
> ***BSI (Germany) - Internet of Things (2021)*** *[German BSI 2021]*

This definition primarily frames IoT within the consumer and smart home space, listing everyday connected products such as wearables and digital assistants. However, Industry 4.0 and smart city technologies are also explicitly referenced, suggesting a broader industrial and enterprise application.

Germany’s IoT discourse frequently ties enterprise and industrial IoT to Industry 4.0 [RTI], the digitisation of manufacturing and industrial processes through connected machines and sensors. While BSI does not explicitly separate EIoT from consumer IoT, its reference to Industry 4.0 reflects the country’s strategic focus on integrating IoT into industrial operations. This aligns with Germany’s broader cyber security priorities, where industrial automation, real-time monitoring and interconnected supply chains require robust cyber security measures to protect critical infrastructure from cyber threats. The BSI’s approach suggests that Germany sees EIoT security as an extension of its industrial security strategy, ensuring that connected factories, logistics networks and business applications remain resilient against emerging digital risks.

Singapore’s Infocom Media Development Authority (IMDA) – Singapore’s ICT regulator, defines IoT technology as:

> *“Internet of Things (IoT) helps to blend the physical environment and objects with traditional Information and Communication Technology (ICT) so that they can interact with one another seamlessly. This technology can be harnessed to improve the quality of life of our citizens, improve efficiency and enable new business models for our enterprises.”*
>
> ***Singapore IMDA – Internet of Things (2023)*** *[IMDA 2023]*

This definition highlights IoT’s role in integrating the physical and digital worlds, enabling automation, connectivity and data-driven interactions across different sectors. While it acknowledges consumer applications focused on enhancing quality of life, it also explicitly recognises IoT’s impact on enterprise innovation and business efficiency.

IMDA emphasises the role of IoT in Singapore’s digital landscape by developing interoperability and cyber security standards to support enterprises. These standards aim to create an ecosystem of secure and interoperable IoT systems that reduce costs and enable data sharing across devices and systems. IMDA’s initiatives such as “SS 695: 2023 IoT interoperability for Smart Nation” and the “IoT Cyber Security Guide (2019)” [IMDA 2023], focus on establishing open interfaces and enhanced security frameworks for the future of IoT devices.

China’s Ministry of Industry and Information Technology (MIIT) published a draft guideline defining IoT in the context of industrial standards as:

> *“The Internet of Things (IoT) can be defined as a network of physical objects embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and*

> *systems over the Internet.”*
> ***China Briefing – China’s Industrial Standards for the Internet of Things (2021)*** *[China Briefing 2021]*

The MIIT’s draft guidelines propose the establishment of a foundational IoT standard system aimed at defining security requirements for all IoT devices. The proposed framework comprises of five major standards: General security, Terminal security, Gateway security, Platform security and Security Management [China Briefing 2021]. This definition encompasses both consumer and EIoT devices and makes sure that all IoT devices are built in a way with security in mind.

The MIIT’s guidelines align with China’s ‘China Standard Plan 2035’ [China Briefing 2022], which in conjunction to the ‘Made in China 2025’ initiative [China Briefing 2018], seeks to modernise industries through IoT, AI and 5G internet. While the definition itself does not explicitly separate EIoT from other IoT applications, its policy context makes it clear that China’s regulatory and industrial focus is on the large-scale deployment of IoT in business and manufacturing, reinforcing IoT use cases in factories and enterprises as a key driver of economic and technological advancement.

A report titled ‘Industry 4.0 Testlabs in Australia written for the Australian Department of Industry, Innovation and Science’ talks about how IIoT connects into enterprise systems:

> *“the IIoT describes systems that connect and integrate industrial control systems with enterprise systems, business processes and analytics. The aim of IIoT is to optimise operations across asset types, fleets, suppliers and customers worldwide.”*
> ***The Prime Minister’s Industry 4.0 Taskforce (2017)*** *[industry.gov.au 2017]*

This definition states how IIoT bridges the gap between industrial control systems and enterprise-level technology to enable data-driven optimisation. It emphasises business process enhancements but does not address key challenges such as cyber security risks that traditionally come with integrating systems together. The paper talks specifically about “OT-IT” convergence [industry.gov.au 2017]. The inclusion of industrial and enterprise systems together under one definition suggests an elevated level of interoperability between the two sectors and that industrial and enterprise systems together play a shared role in increasing business efficiency.

The mention of industrial control systems typically refers to operational technology, but in the context of IoT could mean sensors and actuators. The outputs of these systems then feed into traditional “enterprise” IT systems to then make informed decisions based on the collected data such as predictive maintenance or supply chain adjustments. The 2020 Australian Code of

Practice ‘Securing the Internet of Things for Consumers’ [Australian Government 2020] states that “Consumers may take many forms. Governments, businesses and individuals may all be consumers of IoT devices.”. The document makes no separation between IoT used in homes versus offices. The code of practice goes on further to state that “This group of devices does not include mobile phones – as they are considered sophisticated devices and other guidance may more accurately apply.”, leaving mobile phones out of scope.

The United Nations’ International Telecommunication Union (ITU) defines IoT as:

> *“A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies”*
>
> ***ITU - GSR discussion paper Regulation and the Internet of Things (2015)*** *[ITU 2015]*

While the ITU's definition provides an abstract overview of IoT, it does not explicitly differentiate between any verticals, such as consumer IoT and EIoT. Even though their definition is over a decade old, it is still used in recent work. The organisation had established a Study Group in June 2015 to look at creating standards for IoT. In 2024, Study Group 20 of the ITU released draft guidelines [ITU 2024] defining IIoT, which stated that “Industrial Internet of things (IIoT) infrastructure for smart manufacturing refers to common facilities based on IoT that support smart manufacturing in industries or sectors.”. The majority of the ITU’s work is non-public, so it is not possible to assess if the organisation has since created definitions separating EIoT from IIoT.

Internationally, definitions of IoT associated with enterprise environments mirror the UK’s themes with slight variations in terminology. In the US, emphasis is often on defining the types of products that fall into the categories, for example, definitions highlight interconnected sensors and machines in automation-heavy environment to improve reliability and efficiency [US Congress 2020] [CISA 2021] when specifically, not talking about consumer devices [FCC 2024]. The core concept remains linking devices and analytics to business outcomes, as one US source notes IoT industries “increase efficiency and reliability in their operations, with reduced reliance on human-to-machine interactions” [RTI]. The European Union also defines IoT broadly as networks of smart objects and places particular weight on transformative uses in smart cities and industry (often under the banner of “Industry 4.0”), One notable difference is in regional focus: EU discussions sometimes stress citizen-centric outcomes (for example smarter cities and infrastructure) [Interoperable Europe EC] alongside enterprise efficiency, while US discussions frequently tie IoT into cloud services and AI for accelerated adoption [NIST 2024].

However, subtle but significant differences emerge regarding the scope of devices that are covered. While the various definitions used by UK institutions in their publications tend to focus on connected office equipment that is essential to core business function, the US might exclude or significantly differ on devices such as personal computers and mobile devices from their definitions. Although the outcomes may be similar, the driving force behind them may not be. Each region may prioritise distinct aspects (the UK and EU increasingly highlight security and privacy in IoT definitions due to regulatory drivers, whereas US industry definitions might highlight innovation and return on investmentOI). Each viewpoint contributes to a multifaceted understanding of EIoT, covering technological, business and to some extent societal dimensions.

Common Themes

All the sources emphasise that EIoT is fundamentally about connecting physical "things" to networks to automate business processes. For instance, the NCSC states that EIoT "enables physical 'things' with embedded computing devices to participate in business processes for reducing manual work and increasing overall efficiency" [NCSC 2022]. Similarly, Microsoft categorises EIoT by highlighting devices such as "printers, scanners, cameras, Smart TVs, VoIP phones and other purpose-built devices used to streamline enterprise processes" [Microsoft 2022]. These perspectives consistently portray EIoT to reduce manual intervention and improve operational efficiency.

Several definitions underscore the integration of connected devices into core enterprise operations. The UK Parliament report [UK Parliament 2023] clarifies that while "enterprise IoT" is used in offices, healthcare and transport, it is distinguished from "industrial IoT" which targets manufacturing and large-scale automation. The wording of this distinction is particularly noteworthy as it uses non-assertive terms such as "sometimes" and "often" to describe the category that connected tech falls under, indicating there is no harsh set boundaries between enterprise and industrial.

Major tech players such as AWS emphasise that IoT "facilitates communication between devices and the cloud, as well as between the devices themselves" [AWS 2024]. This focus on cloud connectivity and scalability reflects industry-wide recognition that modern enterprise systems require robust, real-time data exchange and advanced analytics to support digital transformation.

There are both government and industry sources that highlight IoT as "industry-agnostic" – it applies across a broad spectrum of business environments. While Parliament makes a distinction between Enterprise and Industry, using non-assertive terms, there are commonalities that underpin all types of IoT, that cannot be ignored. Whether the IoT is deployed in smart factories, offices, or public service sectors; the underlying principles remain consistent: enhancing efficiency, reducing manual work and enabling data-driven decision making. TechUK's briefing with DCMS reinforces this notion by describing EIoT in terms of common business devices such as office printers, cameras and room booking systems [TechUK 2022].

Gaps in Existing Definitions

While the benefits of EIoT in automation and efficiency are well documented, few definitions explicitly address the factors that create potential dividing lines between types of definition of IoT. Some of these are related to security and privacy challenges. Although Microsoft and the IoTSF acknowledge that integrating IoT devices with business-critical systems introduces new risks, it is not the key factor in most definitions in deciding whether IoT is considered to be in one division (such as EIoT), versus consumer IoT, for example. Definitions by their nature cannot go into detail. It may be that a precursor to deciding what type of IoT sector something is in, also encompasses the deployment context, which often means that security would be a key consideration. This would then imply that the manufacturer and purchaser of such IoT would have to review relevant governance frameworks, product security requirements and privacy safeguards needed to manage the risks that arise from different deployment contexts as increased connectivity broadens the attack surface.

Academic and Industry literature stresses the need for seamless integration of IoT devices with existing enterprise systems such as Enterprise Resource Planning (ERP), Manufacturing Execution Systems (MES) and Operational Technology (OT). However, many official definitions do not elaborate on the technical challenges associated with ensuring interoperability among a diverse range of devices and legacy systems. The complexity of aligning new IoT deployments with established IT infrastructures remains underexplored.

There is notable variation in how sources distinguish between EIoT and IIoT. The UK Parliament report clearly separates them – Identifying EIoT as technology used in offices, healthcare and public services and IIoT as primarily focused on large-scale manufacturing and energy infrastructure [Parliament 2023]. In contrast, other sources such as AWS adopt a broader definition that does not explicitly make this distinction, potentially leading to ambiguity – especially in cases where consumer-grade devices are used in business settings.

Although definitions from IoT service providers such as Microsoft and AWS capture the transformative potential of EIoT in terms of efficiency and automation, they often overlook the importance of managing the entire device lifecycle. Critical aspects such as secure onboarding, continuous updates, network segmentation and eventual decommissioning are seldom mentioned outside of organisations such as the IoTSF. This gap suggests that while operational benefits are acknowledged, comprehensive governance strategies for sustaining secure and reliable IoT deployments are not adequately addressed.

Secondary Market Research of EIoT

Industry landscape

The EIoT market in the UK is diverse and includes a mix of telecom operators, global tech firms and specialised IoT solution providers. Telecom providers play a foundational role by providing IoT connectivity (networks and SIMs) and platform services. For instance, BT (through its mobile arm EE) and Vodafone have each established dedicated IoT networks – BT launched a nationwide Narrowband-IoT (NB-IoT) network covering 97% of the UK population to support smart city, utilities, construction and logistics applications [RCWireless]. Likewise, Vodafone's IoT division connects millions of devices and publishes an "IoT Barometer," indicating its prominence in this space [VBarometer]. Other mobile operators like O2 (Telefónica) [O2] and Three [Three] also offer IoT connectivity services, meaning all major UK carriers are key EIoT enablers.

In addition, IT and technology service providers are pivotal: global companies such as Cisco, IBM and Microsoft are among the top IoT solution vendors in the UK. Cisco provides network IoT platform infrastructure, IBM and Microsoft offer cloud-based IoT platforms (Azure IoT, Watson IoT, etc) [Cisco] [IBM] [Microsoft]. Hardware firms such as Qualcomm and Intel supply IoT chipsets and edge devices [Qualcomm] [Intel]. These firms often partner with local enterprises to deploy IoT projects.

The market also features IIoT specialists in system integrators. Large industrial automation companies like Siemens, Bosch and Schneider Electric, which are global leaders in IIoT, have strong UK presence, delivering IoT-enabled solutions in manufacturing, energy and building management [Siemens] [Bosch] [SE]. Alongside, numerous UK-based startups and niche players contribute innovative solutions – for example, companies specialising in smart sensor networks, IoT device management, or sector specific applications (for example Agri-Tech IoT for smart farming, or telematics firms for vehicle tracking.) The net result is a fragmented ecosystem where no single vendor dominates; instead, collaborations between connectivity providers, platform providers and domain experts are common.

In summary, telecom operators (BT, Vodafone, etc) provide the connectivity backbone, large IT providers (Microsoft, IBM, AWS, etc) offer IoT platforms and integration services and industrial specialists (Siemens, Schneider, etc) deliver vertical-specific IoT systems – together forming the key player landscape of UK EIoT. This mix ensures enterprises in the UK have access to both global innovations and local expertise when adopting IoT.

Current trends and investments

The use of IoT in UK businesses is claimed to be experiencing robust growth, driven by increasing adoption across industries and significant investments in IoT capabilities. According to Vodafone's 'IoT Barometer' [VBarometer], over one-third (34%) of businesses surveyed globally were using IoT by 2019, and this rate has accelerated in recent years. The report shows a strong majority of firms view IoT as strategically important – 76% of businesses say IoT will be critical to their future success, reflecting confidence in IoT's value proposition. This demand is fuelling market growth; one forecast predicts a 15% annual growth rate for the global EIoT market, reaching $690 billion by 2030 [IoTAnalytics]. Major investments are coming from both the private and public sectors. Telecom operators have invested in new networks (as noted, BT's multi-million-pound NB-IoT rollout) [RCWireless] and Vodafone's ongoing expansion of Long Term Evolution for Machines (LTE-M)/NB-IoT coverage) to enable nationwide IoT connectivity. Tech companies investing in UK IoT startups and pilot project – for example, partnerships to bring edge computing and 5G capabilities to IoT solutions (such as BT's collaboration with AWS on 5G edge for IoT [MarketScale].

The UK government has also injected funding to spur IoT adoption as part of its industrial strategy. A notable example is the "Manufacturing Made Smarter" initiative, which in 2020 announced £147 million to boost adoption of industrial digital technologies (IoT, AI, Robotics) in manufacturing, aiming to raise productivity and drive innovation in UK factories [UKRI]. Similarly, the "Made Smarter" program (piloted in regions like Northwest England) provides grants and support for Small and Medium Sized Enterprises (SMEs) to implement IoT and other Industry 4.0 technologies, indicating policy-level investment in EIoT [MadeSmarter].

Another trend is the proliferation of IoT platforms and ecosystems – many enterprises are moving from small pilots to scaled deployments, standardising on platforms from the key players mentioned earlier. This has led to strong demand for IoT integration services (connecting legacy systems with new IoT data streams) and solutions for addressing IoT data analytics and AI (to extract actionable insights from sensor data). Venture capital funding in UK IoT startups (for example in smart sensor, analytics, or device security companies) has grown alongside, though the market remains competitive.

In the 2021, the IoT Security Foundation's annual report titled 'The State of Vulnerability Disclosure Policy (VDP) Usage in Global Consumer IoT' [Copper Horse VDP 2021], was the first edition of it to include discussion on providers of EIoT, termed 'Business-to-Business (B2B)' IoT products. Initial findings uncovered that 71.4% of B2B providers had a disclosure policy in place for reporting vulnerabilities, compared to just 21.6% of Business-to-Consumer (B2C) companies. Over the course of the next three years, the 2024 publication of the 'VDP Usage in the Global Consumer IoT' [Copper Horse VDP 2024] saw this figure rise to 91.6% of B2B manufacturers having a vulnerability disclosure policy in place (an increase of 20.5%). In the same timeframe, disclosure policies for B2C IoT companies rose to 36.59% (an increase of 14.99%). This stark difference between B2B and B2C companies that provide a channel for security researchers to report vulnerabilities shows the increased security considerations given to B2B IoT products. Given the high stakes involved where B2B providers risk significant revenue loss due to compromised trust and the businesses deploying these devices face potential data breaches, it is critical for B2B providers to have the necessary pathways to report vulnerabilities. There is a two and a half times difference in B2B companies over B2C that provide a channel for reporting, underpinning cyber security concerns as a key defining factor between enterprise and consumer IoT.

Overall, the trajectory of the UK EIoT market is one of expansion and maturation: broader adoption, bigger deployments and more money spent on IoT infrastructure. The COVID-19 pandemic provided an extra impetus – with remote monitoring, supply chain visibility and building automation needs rising, many organisations accelerated IoT projects. This increase in adoption also comes with the added risk of “shadow IoT” – devices which are unauthorised or unmanaged within an organisation’s networks [CSO Online 2019]. With these trends, the IoT market in the UK continues to attract investment and analysts from Technavio estimate 11.6% compound annual growth rate over the next 3 years [Technavio 2024], particularly fuelled by the rise in industry 4.0, as IoT becomes a mainstream component in enterprise sectors such as Industrial, Retail, Healthcare and ICT.

Sector-Specific Application of Key Technologies

EIoT in the UK spans all sectors, but adoption is particularly notable in certain industries.

Manufacturing and Industry 4.0,is becoming a leading sector for EIoT deployment. UK manufacturers are implementing IoT on factory floors for predictive maintenance, real-time production monitoring and supply chain optimisation. For example, IIoT sensors are attached to machinery to detect anomalies and schedule maintenance before breakdowns, reducing downtime. “IoT-based predictive maintenance is a transformative approach that combines technology and analytics” driving efficiency improvements in production [ForestRock]. The UK’s automotive and aerospace manufacturers, among others, have embraced IoT to track assets and improve quality (for example aircraft engine makers using IoT data to monitor engine health) [RollsRoyce]. Government-backed testbeds (like the Digital Catapult’s trials) and funding (Made Smarter) specifically target manufacturing IoT, underscoring its importance [DigitalCatapult] [MadeSmarter].

Smart infrastructure and Cities: IoT is being applied to infrastructure management and urban innovation in the UK. “Smart city” initiatives use connected sensors for everything from intelligent street lighting and traffic management to environmental monitoring. The goal is to make infrastructure more efficient, safe and responsive. For instance, cities like London, Manchester and Bristol all run pilots from smart parking (sensors guiding drivers to free spots) to air quality monitoring via IoT devices [GovernmentEvents]. EIoT solutions are crucial in utilities – the nationwide rollout of smart energy meters is a prominent example of IoT infrastructure, bringing millions of connected devices to monitor electricity and gas usage in real-time. In construction and civil engineering, IoT sensors are embedded in bridges or buildings to track structural health. An industry commentary notes that EIoT innovations are making smart cities “cleaner, safer and efficient” [YourStory], illustrating the focus on public safety and resource efficiency. Companies like Siemens and BT work on smart infrastructure projects, integrating IoT platforms with city data systems. These efforts align with broader UK smart infrastructure goals (such as improving transportation networks and utility services via IoT.)

Other sectors: Many other enterprise sectors in the UK are adopting IoT in tailored ways. Retail companies use in-store IoT devices for smart inventory (shelves that detect stock levels) and enhanced customer experiences (for example smart digital signage). Healthcare organisations deploy IoT for patient monitoring and asset tracking in hospitals – UK hospitals are testing IoT wearable sensors and smart equipment to improve patient care and operational efficiency.

Agriculture (smart farming) is another area, with IoT sensors helping UK farms monitor soil conditions and livestock (often referred to as precision agriculture). Finance and Insurance sectors even use IoT data (like telematics data in insurance or smart building sensors for risk assessment). While manufacturing, infrastructure and logistics are flag-bearers, EIoT's influence is multi-sectoral and enterprises across the board are finding use cases that apply to their domain. Each sector tends to have its signature IoT applications – but all share the goals of cost reduction, automation and data insight. It is also worth noting that many IoT deployments overlap sectors: for instance, a "smart city" project can involve transportation (smart traffic lights) and public safety (connected CCTV cameras) which in a business context engages private firms providing those solutions. Literature review on connected devices within enterprise networks – a 2019 study of EIoT found implementations in at least nine categories of industries, with manufacturing, energy/utilities and transport among the top in terms of use-case volume [Ipsos Mori]. This cross-sector presence of EIoT in the UK underscores its versatility and the wide-ranging impact expected from IoT technologies.

Regulatory landscape

The regulatory environment in the UK plays a significant role in shaping EIoT adoption – particularly concerning data protection and device security, which are vital for trust in IoT systems.

The UK introduced one of the world's first IoT-specific security laws – Part 1 of the Product Security and Telecommunications Infrastructure Act 2022 (PSTI) and its associated Regulations – which came into force in April 2024 [PTSI]. This regulatory regime directly impacts the IoT device market by making certain security requirements mandatory. Focused on consumer connectable products, it has implications for enterprise since many devices used in businesses (like office IoT devices, routers, cameras) are also consumer-grade or at least, not industrial-only. Part 1 of the PSTI Act and the associated Regulations set baseline security standards for IoT devices, notably banning universal default or easily guessable default passwords, requiring a means for vulnerability reporting and mandating transparency about how long devices can expect to receive security updates [BCS] [Thales]. It effectively shifts responsibility to manufacturers to build security into IoT products by design [Thales]. For enterprises, this legislation means that over time the IoT products they deploy should come with better built-in security. For others in the supply chain, including importers and distributors, the regime currently obligates them, among other things, to ensure any consumer connectable products they make available to customers in the UK is accompanied with a statement of compliance outlining that the manufacturer considers it compliant with these security standards. Relevant connectable products not available to a private person for purchase , remain outside of the scope of this regime. Although these devices are still legal to use, enterprises should audit their device inventory to ensure the products are set up in a safe and secure manner and ensure they avoid purchasing products that do not comply (for example devices with hard-coded universal default passwords [Thales]). In the long run, PSTI is expected to enhance the overall security of a large number of IoT ecosystems by reducing very commonly exploited vulnerabilities.

The UK's telecom and cyber policies also influence EIoT. Ofcom, the telecoms sector regulator, has worked to ensure sufficient spectrum and reliable networks for IoT services – for example, dedicating spectrum bands for IoT (for example, the use of licensed LTE bands for NB-IoT and unlicensed spectrum for LoRaWAN) and permitting "national roaming" Subscriber Identity Modules (SIMs) to improve coverage [Fast Mode] [LoRaWan]. Initiatives under the 5G strategy also tie in: 5G networks are seen as a catalyst for advanced IoT due to their low latency and massive device support and the UK's 5G trials often incorporate IoT use-cases (such as smart factories or connected transport) [5G IoT]. Prior to Brexit, the UK adopted the Network and Information Systems (NIS) regulations in 2018 [NIS 2018] from the EU. In 2024 the EU enacted NIS2 [NIS2 2024] into law, which superseded the existing NIS regulations. Since leaving the EU, NIS2 would not automatically go into effect in the UK. This led to the plan of creating the Cyber Security and Resilience Bill, which is set to be introduced to Parliament in 2025 and is intended to update the existing NIS regulations that were inherited from the EU. The bill will impose cyber security requirements on operators of essential services – this covers sectors like energy, health, transport and digital infrastructure as IoT systems continue to play an increasingly critical role in their operations [CS&R Bill]. Companies in those sectors must manage cyber risks (including IoT security) and report serious incidents.

Another facet is standards and certifications: In 2018, DCMS had issued IoT security best practices such as the 2018 'Code of Practice for Consumer IoT Security' [CoPfCIoTS], which laid the groundwork for subsequent standards and legislation. In 2020 the European Telecommunications Standards Institute (ETSI) built on top of the 2018 Code of Practice to publish ETSI EN 303 645 [ETSI 2020] as an international standard for consumer IoT security. This then led to development of the Part 1 of the UK's PTSI Act which received Royal Assent in 2022, with associated regulations passed in 2023, to enforce mandatory security requirements for consumer connectable products. While enterprise devices not available to individual consumers are out of scope in these documents, they still create a de facto expectation for IoT deployments. In addition to the international standard from ETSI, other similar work exists (for example from NIST). Businesses also may look for IoT devices certification under schemes such as the BSI Kitemark for IoT [BSI] or adopt the requirements in the assurance framework from the IoT Security Foundation [IoTSF AF], or the GSMA's IoT Security Guidelines, FS.60 [GSMA 2024]. Taken as a whole, all of these initiatives and policies push the EIoT market toward secure and resilient implementation, ensuring that while IoT adoption grows, it does not become the main source for the compromise of data security or network integrity. These government initiatives might increase upfront costs or complexity to meet standards, but it also builds confidence in the security, robustness and resilience of IoT solutions, which is crucial for widespread enterprise uptake.

Expert Insights & Analysis

Findings from Interviews

A PhD researcher suggests the EIoT encompasses connected devices deployed within organisational settings, specifically to enhance efficiency, automate processes and enable data-driven decisions. She emphasises the integration of EIoT within centralised enterprise cyber security and telemetry frameworks, noting significant organisational impacts such as changes to workplace privacy, surveillance and hierarchical structures. She offers a unique analogy, comparing threats from dual-use IoT devices to insider threats, highlighting often-overlooked complexity of IoT in organisational contexts.

A former IoT connectivity professional at a large technology company highlights that EIoT specifically addresses interconnected devices with clear enterprise use cases, explicitly excluding consumer devices such as mobile phones and laptops. Their perspective points out the importance of preserving a clear boundary between consumer IoT and EIoT to maintain definition clarity and practical applicability.

An expert from an IoT security industry body characterises EIoT through scalability, enterprise-grade security and compliance as key defining attributes. He underscores EIoT's role in driving business optimisation, efficiency and analytics-driven decisions, notably highlighting the necessity of distinguishing it clearly from consumer IoT due to higher security and compliance requirements.

A cyber security analyst provided a broader perspective by differentiating between intentional IoT deployments and the unintentional devices connecting within enterprise networks (such as Bring Your Own Device, or BYOD, policies). He addresses the complexity of managing personal devices such as laptops and smartphones within enterprise environments by advocating for their inclusion, highlighting their connectivity and significant security implications as integral elements of modern enterprise ecosystems.

A PhD research student at UCL highlights the complexity and ambiguity in strictly defining EIoT due to the overlapping usage between consumer and enterprise contexts. He suggests adopting a practical and flexible approach to categorisation that better reflects the diverse and evolving nature of device deployment.

One interviewee highlighted the extensive diversity within EIoT, with examples ranging from building management systems to satellites and drones. He argues for a zoological approach to categorisation, grouping devices based on function and technological evolution, criticising rigid, narrow definitions for failing to represent the actual diversity of current IoT implementations.

A VP of Engineering at an IoT company, defines EIoT as connected, autonomous, fixed function devices deployed in substantial numbers by medium to large companies. They emphasised the difference in the scale and operational context between EIoT and consumer IoT, pointing out that EIoT involves expert-driven deployment. They noted a scenario where aviation routers that have default passwords are permissible, but in consumer deployments would be unacceptable. He further distinguishes IIoT as typically factory-based, highlighting its differentiation from the corporate IT associated with EIoT.

An IoT engineering consultant highlighted the difficulty in strictly defining EIoT due to the overlaps between enterprise, consumer and industrial deployments. They questioned the clarity of definitions, particularly criticising the exclusion of OT, which he believes creates unnecessary ambiguity and potential regulatory loopholes. Arguing for context-driven categorisation, citing devices such as printers and laptops as inherently dual-use and emphasising that the security risk lies in their application rather than their inherent design. He also points to broader regulatory and market complexities, including the challenges of enforcing security standards on devices readily available to both enterprises and consumes, thus suggesting the need for adaptable, context-aware definitions.

A Commercial Director in an IoT company described EIoT as interconnected physical devices and sensors that gather data for analytical purposes, particularly focussed on enhancing workplace management and operational efficiency. He emphasises practical use cases, suggesting the IoT's value in an enterprise context lies in enabling business to make informed decisions, such as monitoring workspace utilisation or managing office environment effectively. He specifically questioned the exclusion of OT, given its foundational role in IoT, and highlights overlaps between consumer and enterprise devices, advocating for a flexible, use-case-driven categorisation.

An IoT certification specialist at a technology certification body defines EIoT as connected devices that are autonomous, fixed function and managed centrally within business organisations. He emphasis governance, lifecycle management and stringent security policies as distinguishing factors between enterprise and consumer IoT. One notable comment is the importance of centralised management and regulatory compliance as key elements differentiating enterprise devices from consumer products. He also acknowledges the evolving nature of EIoT, advocating for industry collaboration to refine standards, particularly as consumer-grade devices increasingly enter enterprise environments. This has the potential to create issues in how device manufacturers define what category their product falls under, particularly if one set of standards is less stringent than another.

Validation & Challenges

Experts recognise the utility of existing definitions, such as the one provided by NCSC, acknowledging that these definitions offer helpful policy guidance and baseline frameworks for distinguishing EIoT from consumer and industrial technologies.

However, opinions diverge significantly regarding the scope and practicality of these definitions. Multiple experts criticise the NCSC definition as overly rigid and outdated, particularly for excluding Operational Technology and devices with dual use in consumer markets. They highlight that these exclusions do not accurately reflect the practical reality and integration of modern IoT deployments across different contexts.

Experts agree that printers can qualify as EIoT devices, especially when integrated into organisational workflows and network systems. The consensus is due to their monitoring capabilities and role within enterprise hierarchies.

Conversely, opinions differ sharply regarding laptops. Some of them argue against including laptops, seeing them primarily as computing devices rather than IoT. Meanwhile, another expert views laptops as part of the EIoT landscape due to their connectivity and management complexity. This difference underscores the complexity of clearly defining IoT in the evolving enterprise landscape.

Consensus emerges among several experts that mobile devices introduce complexity to the definition of EIoT, especially concerning corporate-owned versus BYOD scenarios. Experts recognise the grey area created by BYOD policies, complicating security and compliance management. The main difference is whether mobile devices inherently qualify as IoT. One expert firmly excludes them, viewing them primarily as communication devices. However, another argues their connectivity and associated risks justify their inclusion within a broader EIoT definition.

Enterprise IoT vs Consumer IoT – Experts universally agree on several key distinctions between enterprise and consumer, primarily emphasising differences in purpose, management, security requirements and operational complexity. A common consensus is that EIoT is characterised by centrally managed deployments within organisational frameworks, often governed by strict cyber security and compliance directives such as the UK General Data Protection Regulation (GDPR). EIoT typically supports operational efficiency, decision-making and process automation, contrasting sharply with consumer IoT, which is simpler, user-managed and designed for personal convenience and entertainment.

However, differences in opinion arise around the categorisation of specific devices due to their dual-use nature. For instance, while security cameras and printers are recognised as existing in both domains, some experts highlight the scale, management and integration complexity are substantially different in enterprise context. One expert adds another layer by noting that EIoT inherently carries greater risk due to the sensitivity of organisational data, as opposed to consumer settings where the risks and associated security measures are often less stringent. Despite consensus on the broad differences, experts acknowledge the boundary between consumer and EIoT remains complex and often blurred, necessitating flexibility in categorisation.

Experts identify clear distinctions between IIoT and EIoT, emphasising differences in operational context, priorities and regulatory requirements. IIoT is typically defined by its emphasis on real-time operational control, high reliability and stringent security, particularly because device failure in IIoT scenarios – such as manufacturing or critical infrastructure – can lead to significant disruptions or safety risks. Conversely, EIoT is more strongly associated with enhancing organisational decision-making, business process optimisation and data analytics. Two of them specifically highlight these differences, noting that IIoT solutions often require bespoke, sector-specific technology with a higher standard of reliability compared to general enterprise deployments.

In regulated sectors such as healthcare and automotive, experts acknowledge the distinct position these sectors hold within the broader EIoT landscape. Devices within these industries frequently face rigorous regulatory compliance and testing standards due to their direct impact on human safety and wellbeing. Three of them collectively recognise the heightened security requirements and operational risks associated with IoT deployments in healthcare and automotive sectors. They note that while these industries are fundamentally enterprise environments, their IoT deployments require additional considerations that set them apart from typical EIoT scenarios, further complicating the definition boundaries.

All experts strongly agree that interoperability represents a critical requirement that is inadequately addressed in existing definitions, unanimously highlighting this as a significant practical challenge. One notably underscores interoperability as crucial for unlocking EIoT's full potential. No significant divergence was observed regarding interoperability, suggesting universal expert agreement that interoperability is a major challenge currently overlooked or under-addresses in definitions.

Experts agree on the necessity of adopting flexible, adaptive definitions capable of accommodating future technological advancements and emerging device categories. One even specifically advocates for dynamic definitions, criticising current approaches as static and unable to accommodate the rapidly evolving IoT landscape. There was clear consensus demonstrating collective support for future-proof, adaptable frameworks for defining EIoT.

A Definition of Enterprise IoT

A definition of Enterprise IoT may, at this point, be the wrong thing to ascertain, as there is no universally understood division between other market segments. Governments are already directly opposed in their view to what constitutes IoT with the US and the UK differing on their views on PCs as IoT, as an example.

It is tempting to state ‘any business usage of IoT' i.e., the defining line is drawn at the acquisition of an IoT product or solution by a business. However, this definition would immediately encompass any existing regulated domains (such as medical) and also include all factory floor or production equipment usage (OT). It is unlikely that a clean separation of OT and enterprise is possible, without significantly disrupting how industries and factories operate; and for little gain in terms of real-terms security, safety or other context-specific factors.

The compounding factor in government intervention in securing the internet of things is the existing artificial segmentation of the market for IoT products. This is coupled with government departmental segmentation of sectors. These lines are arbitrary in many cases, either historical divisions or organic, but they create significant grey areas for dividing up technology. At the moment, governments can distinguish between some sectors of IoT based on pre-existing standards and regulatory intervention which have been driven by safety (for example in the case of medical devices or vehicles), but these lines are increasingly blurred. ‘Wellness' devices for consumers are very close to being medical devices and their practical usage demonstrates that. The same applies in the enterprise domain. Small businesses buy products from consumer-focused retail stores – for example printers, smart large screens and cameras. This also extends to large businesses – for example, hotels will often buy TVs that were destined for the consumer market. Artificially dictating the lines by which these products are sold could be damaging to the free market, overbearing and costly. Hence, there appears to be more negatives than positives, with no obvious gain for business or in the domain of cyber security.

If a definition did exist and it were used for future governance of security (even regulatory), companies may seek to deliberately avoid meeting more stringent security requirements where there are ambiguities. This would create significant cost and operational challenges for all stakeholders and, if it were regulated, become a nightmare for the appointed regulator who would need to go through multiple legal challenges to rulings in ambiguous areas.

How is this conundrum solved? It is true that the threat to all IT systems and IoT has increased as the world has become more connected. No business or consumer is going to deny that there is a need for security in all connected devices. Indeed, there is a general expectation that products that are purchased are 'secure' and continue to be so.

Conversely, individual sector-specific 'vertical' requirements may fragment the market and again present opportunities for unscrupulous behaviour in order to avoid more stringent security requirements. The need to create additional security for specific contexts or applications is not going to disappear. The traditional way of dealing with this was for companies to be required to perform a security risk and threat analysis. This is in order to elicit the security requirements that are needed to secure a particular product, service or solution in a particular environment. This again leaves gaps – many companies do not know how to perform a risk and threat analysis, others 'game' the system by deliberately constraining the scope of their analysis in order to avoid (perceived) costly product and other information security measures. Others wait until their system is developed before attempting to write a threat and risk analysis document which retrofits to their solution. This is a persistent issue which is compounded by many international standards which often require a risk and threat analysis to be produced, leaving the implementation specifics to the user, allowing companies to cherry-pick security requirements with little oversight or consequences. This area requires further study by government.

Policy Recommendations

It is clear from the research conducted in this report that there is no universal definition of enterprise IoT and that there are significantly differing opinions over whether it fundamentally should be defined at all. This illustrates one of the significant challenges of all types of Internet of Things solutions and devices. They are becoming pervasive in every sector of life whether it be business or personal usage. Many solutions available on the market are designed to be multi-purpose and the connected products themselves span from small temperature sensors with low, embedded-compute up to very complex systems with many different sensors and actuators.

From a security standpoint this represents a significant challenge. Deployment context is crucial to understanding the risk that may be posed to the connected product or solution. Factors such as the physical environment lead to product robustness and resilience requirements, as well as functional safety requirements in some cases. These may further lead to security requirements too as the deployment context may create a situation where compromise or unauthorised manipulation of a connected device may lead to a human safety problem.

Business and existing IT security control requirements (some required by legislation) may dictate equipment and purchasing decisions, but that is also an assumption about the size of an enterprise. Most small enterprises would not have the financial and human resources available or knowledge to think about such things, they generally have more important things to deal with for their core business activities.

There are some existing security standards which cover spaces where IoT is deployed, for example in the medical context in the US, UL-2900 series standards apply, which cover many aspects of device and solution security. The same applies in the industrial space with the ISA/IEC 62443 standard set, particularly 4-2 [ANSI/ISA 62443 4-2 2018] which covers product security. These examples are illustrative and many others exist.

Many of these standards' requirements are common across different sectors. After all, the physical computing products are all based on a Printed Circuit Board (PCB), with some hardware chips, running some software and connected to a network (or networks). These common aspects cannot be ignored because they also offer an opportunity to harmonise on the basic and foundational requirements that would apply to any device whether it is in the consumer space or a chemical plant.

A common theme in IoT has been a lack of basic security requirements in devices. The issues these lead to account for many of the security breaches that are seen in the media. Therefore, at a general level, all connected products and IoT solutions should meet a higher level of security than they currently, or previously, have done because it has been demonstrably inadequate in all sectors. Currently, the UK government has taken a global lead in mandating requirements for the consumer space, where the problems of insecure IoT have manifested themselves in multiple ways. However, the gap now (as one interview respondent pointed out) means that there is no current way of preventing a business from selling products with hard-coded default passwords into the enterprise space, yet that same business would be subject to substantial fines if they did the same in the consumer space.

But what about the connected lightbulb? This is a good product to study because it can be deployed in every single sector or market segment of IoT. The implementation of network security in a lightbulb is a hard problem because it is a small device, it is physically exposed, it is long-lived and relatively cheap. Some lightbulbs may be IP65 rated for water resistance or have fire-resistance properties. Some may connect to a network directly or indirectly using internet protocol (IP), others via short-range wireless protocols such as Bluetooth™ through another hub device. How does an organisation make a purchasing decision about these when it comes to security? Only they know what environment and context the lightbulb is going into and they might also misjudge the risk. Additionally, there are many different types of products that exist in a single category – an industrial, embedded PC designed for use in a dusty environment may be significantly different to a small desktop PC and the operating system may be hardened either out-of-the-box or by configuration. The same applies to many other products.

In terms of security, it is recommended that the government adopts a core baseline security approach across the whole of IoT, with functionally equivalent standards being recognised in specific domains where they already exist, for example in the area of OT or in medical devices. Identifying domains where standards do not exist but are clearly necessary is an area for further study.

References

[NCSC 2022] National Cyber Security Centre. ‘Threat report on enterprise connected devices’ (2022) (accessed March 2025) https://www.ncsc.gov.uk/files/Threat-report-on-enterprise-connected-devices.pdf

[Ofcom 2020] Ofcom. ‘Improving spectrum access for Wi-Fi – spectrum use in the 5 and 6 GHz bands’ (2020) (accessed March 2025) https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-2-6-weeks/189812-improving-spectrum-access-for-wi-fi----spectrum-use-in-the-5-and-6-ghz-bands/associated-documents/6ghz-statement.pdf?v=325088

[TechUK 2022] TechUK. ‘DCMS/techUK Roundtable – Enterprise IoT and Connected Device Security’ (2022) (accessed March 2025) https://www.techuk.org/what-we-deliver/events/dcms-techuk-roundtable-enterprise-iot-and-connected-device-security.html

[UK Parliament 2023] UK Parliament. ‘Connected tech: smart or sinister?’ (2023) (accessed March 2025) https://publications.parliament.uk/pa/cm5803/cmselect/cmcumeds/157/report.html

[Microsoft 2022] Microsoft. ‘Microsoft Defender for IoT’ (2022) (accessed March 2025) https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-iot

[AWS 2024] Amazon Web Services. ‘What is IoT?’ (2024) (accessed March 2025) https://aws.amazon.com/what-is/iot/

[GOV.UK 2021] GOV.UK. ‘Research on Enterprise IoT Security’ (2021) (accessed March 2025) https://www.gov.uk/government/publications/research-on-enterprise-iot-security

[IoTInsider 2022] IoT Insider. ‘Gov UK offers £200,000 to test security of smart devices’ (2022) (accessed March 2025) https://www.iotinsider.com/news/gov-uk-offers-200000-to-test-security-of-smart-devices/

[PETRAS-IoT 2024] PETRAS-IoT. ‘PETRAS: The National Centre of Excellence for IoT Systems Cybersecurity’ (2024) (accessed March 2025) https://petras-iot.org/

[IoTSF 2018] IoT Security Foundation. ‘IoT Security Architecture and Policy for the Enterprise: A Hub-Based Approach’ (2018) (accessed March 2025) https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Security-Architecture-and-Policy-for-the-Enterprise-a-Hub-Based-Approach.pdf

[Chehri and others 2021] Chehri A and others. ‘Theory and Practice of Implementing a Successful Enterprise IoT Strategy in the Industry 4.0 Era’ Procedia Computer Science (2021): volume 192, pages 4609-4618 (accessed March 2025) https://www.sciencedirect.com/science/article/pii/S1877050921019785

[Gunadham 2024] Gunadham. ‘Designing Enterprise Internet of Things Systems’ International Journal of Information and Knowledge Management (2024): volume 14, number 2 (accessed March 2025) https://ijikm.uitm.edu.my/pdf/v14n2/3_14208.pdf

[US Congress 2020] US Congress. ‘IoT Cybersecurity Improvement Act of 2020’ (2020) (accessed March 2025) https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf

[FCC 2024] Federal Communications Commission. ‘Cybersecurity Labeling for Internet of Things’ Federal Register (2024) (accessed March 2025) https://www.govinfo.gov/content/pkg/FR-2024-07-30/pdf/FR-2024-07-30.pdf

[CISA 2021] Cybersecurity and Infrastructure Security Agency. ‘Securing the Internet of Things (IoT)’ (2021) (accessed March 2025) https://www.cisa.gov/news-events/news/securing-internet-things-iot

[ENISA 2018] European Union Agency for Cybersecurity. ‘Good practices for security of IoT in the context of smart manufacturing’ (2018) (accessed March 2025) https://www.enisa.europa.eu/sites/default/files/publications/WP2018%20O-1-1-1%201%20Good%20practices%20for%20security%20of%20IoT.pdf

[German BSI 2021] Federal Office for Information Security (BSI). ‘Internet of Things – Smart Living’ (2021) (accessed March 2025) https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Internet-der-Dinge-Smart-leben/internet-der-dinge-smart-leben_node.html

[IMDA 2023] Infocomm Media Development Authority. ‘Internet of Things’ (2023) (accessed March 2025) https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/it-standards-and-frameworks/internet-of-things

[China Briefing 2021] China Briefing. ‘China’s Industrial Standards for the Internet of Things: Draft Guidelines Released’ (2021) (accessed March 2025) https://www.china-briefing.com/news/china-internet-of-things-industrial-standards-draft-guidelines-released-5-major-standards/

[China Briefing 2022] China Briefing. ‘China Standards 2035 Strategy: Recent Developments and Their Implications for Foreign Companies’ (2022) (accessed March 2025) https://www.china-briefing.com/news/china-standards-2035-strategy-recent-developments-and-their-implications-foreign-companies/

[China Briefing 2018] China Briefing. ‘Made in China 2025 Explained’ (2018) (accessed March 2025) https://www.china-briefing.com/news/made-in-china-2025-explained/

[industry.gov.au 2017] Department of Industry, Innovation and Science (Australia). ‘Industry 4.0 Testlabs in Australia’ (2017) (accessed March 2025) https://www.industry.gov.au/sites/default/files/July%202018/document/pdf/industry-4.0-testlabs-report.pdf

[Australian Government 2020] Australian Government. ‘Code of Practice: Securing the Internet of Things for Consumers’ (2020) (accessed March 2025) https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

[ITU 2015] International Telecommunication Union. ‘Regulation and the Internet of Things’ (2015) (accessed March 2025) https://www.itu.int/en/ITU-

D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf

[ITU 2024] International Telecommunication Union. 'Industrial Internet of Things (IIoT) Infrastructure for Smart Manufacturing' (2024) (accessed March 2025) https://www.ietf.org/lib/dt/documents/LIAISON/liaison-2024-07-26-itu-t-sg-20-ietf-ls-on-the-consent-of-draft-recommendation-itu-t-y4228-ex-yiiot-infra-sm-fr-requirements-and-framework-of-indus-attachment-1.pdf

[NIST 2024] National Institute of Standards and Technology. 'Draft IoT Advisory Board Report' (2024) (accessed March 2025) https://www.nist.gov/system/files/documents/2024/06/13/Draft%20IoTAB%20Report%2020240613.pdf

[RTI] Real-Time Innovations. 'The IIoT Primer' (accessed March 2025) https://www.rti.com/blog/the-iiot-primer

[Interoperable Europe EC] European Commission. 'Smart Cities and Communities: Technologies and Services for Smart and Efficient Energy Use' (2024) (accessed March 2025) https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation/smart-cities-and-communities-technologies-and-services-smart-and-efficient-energy-use-0

[RCWireless] RCR Wireless. 'BT launches multi-million-pound NB-IoT network for UK smart cities' (2024) (accessed March 2025) https://www.rcrwireless.com/20240223/internet-of-things/bt-launches-multi-million-pound-nb-iot-network-for-uk-smart-cities-etc[VBarometer] https://www.vodafone.com/business/news-and-insights/white-paper/vodafone-iot-barometer-2019

[IBM] IBM. 'Internet of Things' (2023) (accessed March 2025) https://www.ibm.com/think/topics/internet-of-things

[O2] O2. 'IoT Solutions' (2021) (accessed March 2025) https://www.o2.co.uk/business/solutions/o2-iot-solutions

[Three] Three Group Solutions. 'IoT Solutions' (2023) (accessed March 2025) https://groupsolutions.three.com/iot

[Cisco] Cisco Systems. 'Extended Enterprise – Internet of Things (IoT)' (2024) (accessed March 2025) https://www.cisco.com/c/en/us/solutions/internet-of-things/extended-enterprise.html

[Microsoft] Microsoft. 'Azure IoT Solutions' (2024) (accessed March 2025) https://azure.microsoft.com/en-us/solutions/iot

[Qualcomm] Qualcomm. 'Internet of Things' (2024) (accessed March 2025) https://www.qualcomm.com/products/internet-of-things

[Intel] Intel. 'Internet of Things (IoT) Solutions' (2024) (accessed March 2025) https://www.intel.com/content/www/us/en/internet-of-things/overview.html

[Siemens] Siemens. ‘Siemens Industrial IoT – Spark for the IT-OT Fusion’ (2024) (accessed March 2025) https://www.siemens.com/global/en/products/automation/topic-areas/it-ot-convergence/siemens-iiot.html

[Bosch] Bosch. ‘Bosch IoT Suite’ (2024) (accessed March 2025) https://bosch-iot-suite.com/[SE] https://www.se.com/uk/en/work/campaign/innovation/overview.jsp

[IoTAnalytics] IoT Analytics. ‘Enterprise IoT Market Size Reached $269 Billion in 2023, with Growth Deceleration in 2024’ (2024) (accessed March 2025) https://iot-analytics.com/iot-market-size/

[MarketScale] Litwin, Daniel. ‘The UK Just Got an IoT Level-Up. Here’s Why the BT Partnership with AWS is Set to Improve Mission Critical IoT’ (2023) (accessed March 2025) https://marketscale.com/industries/industrial-iot/the-uk-just-got-an-iot-level-up-heres-why-the-bt-partnership-with-aws-is-set-to-improve-mission-critical-iot/

[UKRI] UK Research and Innovation. ‘£147 million investment in Manufacturing Made Smarter’ (11 September 2020) (accessed March 2025) https://www.ukri.org/news/147-million-investment-in-manufacturing-made-smarter/

[MadeSmarter] Made Smarter. ‘Adoption Programme’ (2025) (accessed March 2025) https://www.madesmarter.uk/adoption/

[Copper Horse VDP 2021] Copper Horse. ‘The Contemporary Use of Vulnerability Disclosure in IoT – IoTSF Report’ (2021) (accessed March 2025) https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/The-Contemporary-Use-of-Vulnerability-Disclosure-in-IoT-IoTSF-Report-4-November-2021.pdf

[Copper Horse VDP 2024] Copper Horse. ‘The State of Vulnerability Disclosure Policy (VDP) Usage in Global Consumer IoT in 2024’ (November 2024) (accessed March 2025) https://copperhorse.co.uk/wp-content/uploads/2024/11/The-State-of-Vulnerability-Disclosure-Usage-in-Global-Consumer-IoT-in-2024.pdf

[CSO Online 2019] Martin, James. ‘What is Shadow IoT? How to Mitigate the Risk’ (2019) (accessed March 2025) https://www.csoonline.com/article/566977/what-is-shadow-iot-how-to-mitigate-the-risk.html

[Technavio 2024] Technavio. ‘IoT Market in UK 2024-2028’ (October 2024) (accessed March 2025) https://www.technavio.com/report/iot-market-in-uk-2024-2028

[Helpnet] Vickers, Bob. ‘Happy Birthday GDPR: IoT Impact and Practical Tips for Compliance’ (May 2021) (accessed March 2025) https://www.helpnetsecurity.com/2021/05/25/gdpr-compliance-iot/

[ForestRock] Forest Rock. ‘IoT-Driven Predictive Maintenance: The Key to Reducing Operational Costs’ (February 2025) (accessed March 2025) https://www.forestrock.co.uk/blog/iot-driven-predictive-maintenance/

[DigitalCatapult] Digital Catapult. ‘About Us’ (2025) (accessed March 2025) https://www.digicatapult.org.uk/about/[RollsRoyce] https://www.rolls-royce.com/country-sites/sea/our-stories/2019/delivering-better-engine-performance-with-iot.aspx

[GovernmentEvents] Government Events. ‘The UK’s Top 3 Smart Cities: A Transformative Approach for Local Governments’ (August 2024) (accessed March 2025) https://www.governmentevents.co.uk/ge-insights/the-uks-top-3-smart-cities-a-transformative-approach-for-local-governments/

[YourStory] Juneja, Preeti. ‘These IoT Companies Are Helping Indian Cities Become Smart’ (December 2017) (accessed March 2025) https://yourstory.com/2017/12/iot-companies-helping-india-cities-become-smart

[Ipsos Mori] Ipsos MORI. ‘Literature Review on Connected Devices within Enterprise Networks’ (March 2021) (accessed March 2025) https://assets.publishing.service.gov.uk/media/627509cbd3bf7f5e40ac7ff4/Literature_review_on_connected_devices_within_enterprise_networks.pdf

[UK GDPR] European Union. ‘Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)’ (2016) (accessed March 2025) https://www.legislation.gov.uk/eur/2016/679/contents

[PTSI] UK Government. ‘Product Security and Telecommunications Infrastructure Act 2022’ (2022) (accessed March 2025) https://www.legislation.gov.uk/ukpga/2022/46/contents

[BCS] Harding, James. ‘Navigating the New UK IoT Legislation’ (March 2024) (accessed March 2025) https://www.bcs.org/articles-opinion-and-research/navigating-the-new-uk-iot-legislation/

[Thales] Thales. ‘IoT Cybersecurity: EU, US and UK Regulations’ (January 2024) (accessed March 2025) https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations

[Fast Mode] The Fast Mode. ‘BT Launches IoT National Roaming’ (2023) (accessed March 2025) https://www.thefastmode.com/technology-solutions/30494-bt-launches-iot-national-roaming

[LoRaWAN] Cyngor Gwynedd. ‘The Internet of Things (IoT) with LoRaWAN’ (2023) (accessed March 2025) https://democracy.gwynedd.llyw.cymru/documents/s41438/APPENDIX%2003.pdf

[5G IoT] GSMA. ‘5G IoT’ (2024) (accessed March 2025) https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/5giot/

[NIS 2018] UK Government. ‘The Network and Information Systems Regulations 2018’ (2018) (accessed March 2025) https://www.legislation.gov.uk/uksi/2018/506/contents

[NIS2 2024] European Union. ‘Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the

Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)' (December 2022) (accessed March 2025) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

[CS&R Bill] Department for Science, Innovation and Technology. 'Cyber Security and Resilience Bill' (2024) (accessed March 2025) https://www.gov.uk/government/collections/cyber-security-and-resilience-bill

[CoPfCIoTS] Department for Digital, Culture, Media & Sport. 'Code of Practice for Consumer IoT Security' (October 2018) (accessed March 2025) https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

[ETSI 2020] European Telecommunications Standards Institute. 'ETSI EN 303 645: Cyber Security for Consumer IoT' (2020) (accessed March 2025) https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[BSI] British Standards Institution. 'The BSI Kitemark™ for The Internet of Things' (2018) (accessed March 2025) https://www.bsigroup.com/globalassets/localfiles/en-ae/iot/km-iot-factsheet-web.pdf

[IoTSF AF] IoT Security Foundation. 'IoT Security Assurance Framework Release 3.0' (November 2021) (accessed March 2025) https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf

[GSMA 2024] GSMA. 'IoT Security Guidelines Overview (FS.60)' (April 2024) (accessed March 2025) https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/wp-content/uploads/2024/07/FS.60.pdf

[UL 2023] UL Solutions. 'Medical Device Cybersecurity Standards and Services' (2023) (accessed March 2025) https://www.ul.com/insights/medical-device-cybersecurity-standards-and-services

[ISA/IEC 62443 4-2 2018] International Electrotechnical Commission. 'IEC 62443-4-2: Security for Industrial Automation and Control Systems – Part 4-2: Technical Security Requirements for IACS Components' (2019) (accessed March 2025) https://webstore.iec.ch/publication/34421

Appendix – Interview Details

Total Interviews Conducted: 10

Format:

- individual interviews: 10
- mode:
  - online (video call): 9
  - face-to-face: 1

participant breakdown by sector:

- academia: 2
- industry (IoT/engineering/commercial): 5
- consultant/analysts: 2
- standards/certification bodies: 1

Participant Overview (non-disclosive)

The interviewees included a diverse representation of the IoT ecosystem, including:

- academics from leading UK universities
- industry professionals from IoT solution vendors and engineering firms
- consultants and analysts specialising in IoT cybersecurity
- representatives from standards/certification bodies focussed on IoT governance

Outreach:

- contact was attempted with five additional experts from global tech companies, academic institutions and standards bodies, but they did not respond to the requests for interview

Appendix – Interview Questions

The following question structure was used during the semi-structured expert interviews.

- What is your definition of Enterprise IoT (EIoT)?

- Do you agree with the NCSC definition of Enterprise Connected Device?

  - *Threat-report-on-enterprise-connected-devices-web.pdf:*
    "For the purpose of this paper, Enterprise IoT devices and distinct ECDs are defined as devices that are industry-agnostic and are typically not available or intended for consumers to purchase. Operational Technology (OT) is not within scope "

  - Do you think Printers are Enterprise IoT devices?

    - Why?

  - Do you think Laptops are Enterprise IoT devices?

    - Why?

  - Where do you see mobile devices fitting into the Enterprise IoT landscape?

    - What about BYOD?

- How do you think Enterprise IoT is different to Consumer IoT?

  - What about security cameras? Is that a grey area based on scale of building being monitored?

- How does Industrial IoT fit into the EIoT picture?

- And how do IoT devices in regulated industries like healthcare IoT and automative IoT fit in with Enterprise IoT?

- What other bodies have defined Enterprise IoT?

- Who else should we speak to?

- Any other views or opinions on EIoT that we have not discussed?