Department for Science, Innovation & Technology

Call for Views on the Cyber Security of Enterprise Connected Devices

Ministerial Foreword

Feryal Clark, Parliamentary Under-Secretary of State for AI and Digital Government

As set out in the Government response to the Call for Views on the Cyber Security of AI it is a priority for HMG to ensure that all new and existing technologies are safely developed and deployed across the UK. The UK, as a world leader in securing technology, will continue to advocate the importance of cyber security and the need for a secure by design approach across all technologies.

Connected devices, often referred to as Internet of Things (IoT), have revolutionised the way we work. In a modern office, everything from the printer to the conference tables can connect to an organisation's network or directly to the internet. It is vital that we unlock the power of these devices across the whole economy and enable businesses to continue to benefit from the increased productivity and efficiency they offer. The growth of the connected device market is undeniable. Forecasts suggest that the global IoT market will grow to 24.1 billion devices by 2030, generating over £1.1 trillion annual revenue.[1] With adoption on the rise, we must ensure that these devices are designed with greater security to protect organisations from cyber attacks. All it takes is a single vulnerable device to expose an organisation to attack. This can lead to loss of sensitive data, disruption of services, financial loss or, in the worst-case scenario, physical harm or death.

Enterprise connected devices remain a hugely attractive target for cyber criminals and our adversaries as many of these devices have limited security features built in, making them an easy target. One hacking group in 2016 compromised Voice over Internet Protocol (VoIP)

[1] Transforma Insights, (2020), Global IoT market to grow to 24.1 billion devices in 2030.

networks of almost 1,200 organisations in over 20 countries, with over half the victims being in the UK.[2]

Threat actors can also leverage the computing power of compromised enterprise connected devices to carry out Distributed Denial of Service (DDoS) attacks that have the potential to cause widespread disruption or bring down essential services. The 2016 Mirai botnet attack infected hundreds of thousands of connected devices to launch a massive attack that brought down websites such as Twitter, the Guardian, Netflix and many others in Europe and the US.[3] DDoS attacks are widespread and remain prevalent because criminals are still able to exploit common vulnerabilities such as weak passwords or outdated software.

This is why we have already encouraged industry to act. In April 2024, the UK's world leading product security regulatory regime came into force, mandating important baseline cyber security requirements for "consumer connectable product". We must now act to ensure that connected devices used in a business context are also afforded better protection throughout their lifecycles.

I am therefore pleased to announce this Call for Views on the Cyber Security of Enterprise Connected Devices. The government is proposing a two-part intervention, including the publication of a Code of Practice and several policy interventions that are being considered to boost uptake of important security requirements.

Engaging with experts, the public, academics and industry remains a crucial part of our ambition to secure the UK's industries and push forward our mission to protect our digital economy and deliver growth. Your engagement with this Call for Views will help the government develop and take forward efforts to build a safer UK.

[2] https://www.ncsc.gov.uk/report/organisational-use-of-enterprise-connected-devices
[3] https://www.bbc.co.uk/news/technology-37738823

Chapter 1: Executive Summary

In May 2022, The Department for Science, Innovation and Technology (DSIT), in conjunction with the National Cyber Security Centre (NCSC), the UK's technical authority on cyber threats, created 11 principles to guide manufacturers in the secure design of enterprise connected devices. This work was in response to growing concerns about the impact of the increased exposure to cyber-attacks faced by organisations because of vulnerable connected devices. These principles were primarily aimed at manufacturers as they are uniquely positioned to drive security across the whole supply chain. Unfortunately, awareness and uptake of these principles has remained low.

This government is aware of the benefits these devices offer and the risks they represent if left unsecured. In recent years we have bolstered our evidence base by conducting research and threat analysis. This work has highlighted significant shortcomings in the security of some connected devices on the market, at all price points. Similarly, security remains an afterthought with approximately 58% of UK businesses not requiring any security or procurement checks when purchasing new connected devices.[4] Many commonly available devices used by organisations in the UK do not contain adequate security features, can have outdated software embedded in them, and possess generally insecure configurations of features[5]. [All this leaves organisations at greater risk of attack.

The government is proposing to turn the principles into a new voluntary Code of Practice for Enterprise Connected Device Security based on the feedback received through this Call for Views. The proposed Code of Practice will then be used as the foundation of a series of proposed policy interventions, of which one or all may be taken forward. We are asking for views on the proposed interventions and are open to suggestions of any other interventions that would help improve the cyber security of enterprise connected devices.

All cyber security Codes of Practice produced by DSIT are part of the government's broader approach to improve baseline cyber security practices and cyber resilience across the UK. A modular approach has been developed to help organisations easily identify which codes and guidance, such as Cyber Governance and Software Vendors codes, are relevant to them according to the types of technologies they either use or manufacture.

Improving the cyber security of enterprise connected devices requires international collaboration, given the global nature of supply chains. This publication is therefore the beginning of extensive dialogue with stakeholders, including manufacturers, key sectors in industry, cyber security experts, academics and international partners.

This Call for Views will run for eight weeks from 12th May to 7th July to gather feedback on the proposed interventions. All interested parties are encouraged to respond to this Call for Views via the online survey form. Please see Annex A for the full Call for Views Survey Questionnaire. Instructions and guidance on how to complete the questionnaire can be found at the beginning of the relevant section of this document. Feedback from all parties will be vital in informing the UK government's policy approach.

[4] https://assets.publishing.service.gov.uk/media/627918bdd3bf7f5e418e0af4/Enterprise_connected_devices_-_procurement__usage_and_management_among_UK_businesses.pdf

[5] NCC Group. 2024. *DSIT Enterprise IoT Product Assessment*.

Chapter 2: Definition of Enterprise Connected Devices

We have defined enterprise connected devices as those used by organisations and/or their employees to process or hold an organisation's data.

Devices that fall within scope of this definition include, but are not limited to:

- Enterprise printers
- Video conferencing systems
- VoIP phones
- Network attached storage (NAS) devices
- Room booking displays

We are currently working on analysing which devices or product types should fall out of scope of this definition.

Chapter 3: Code of Practice for Enterprise Connected Device Security

The proposed voluntary Code of Practice for Enterprise Connected Device Security has been developed based on principles co-authored by the National Cyber Security Centre (NCSC) and DSIT. The Device Security Principles for Manufacturers was published in May 2022 after engagement with industry stakeholders and a beta release in June 2021.

The proposed Code of Practice below is intended to guide manufacturers in the design and creation of secure enterprise connected devices. It aligns with DSITs wider approach to creating baseline security requirements within critical and emerging technologies by establishing clear expectations for cyber security and resilience. The Code of Practice contains 11 broad principles, each with supplementary guidelines to help manufacturers implement simple and effective practices and help organisations gain confidence that enterprise connected devices are protected against common cyber security threats and risks. These principles can also be used by those procuring these devices, offering IoT solutions and/or services to make more informed decisions when purchasing or procuring devices.

The Product Security Regulatory Regime already requires manufacturers of "consumer connectable products" to ensure that their devices adhere to important cyber security requirements. However, the risks posed to organisations and the wider economy by vulnerable connected devices are considerable and therefore these devices require a higher baseline level of security. Therefore, where a device falls in scope of the product security regulatory regime and this proposed Code of Practice, adherence with the principles in this Code, in addition to regulatory obligations, will provide a vital additional level of security. The principles outlined below consider the different capacity for organisations to implement security practices in their network, their broader attack surfaces, and potential to possess data of a higher value. Compliance with this code does not absolve any businesses from the obligations they have under UK law.

We invite stakeholders to provide feedback on the content of this proposed Code of Practice and its supplementary guidelines. It is important to note that the security principles outlined below are not listed in a priority order and do not contain the full guidance and references. Adjacent principles are often related so that it becomes easier for manufacturers to create a coherent narrative if they choose to produce a transparency report.

Code of Practice for Enterprise Connected Device Security

(Each guideline applies to all devices unless explicitly stated)

Language:

- *Shall: Guidelines that specify 'shall' are essential for a manufacturer to claim that they meet the overall principle.*
- *Should: Guidelines that specify 'should' means there may be legitimate reasons why a guideline is not required.*
- *Can: Guidelines that specify 'can' are not considered crucial security features.*

1. **Provide updates, securely.**

Security updates, or patches, are crucial for devices to remain secure throughout their lifespan. This includes both dedicated security updates and feature updates containing security fixes. It is common for vulnerabilities to be discovered in a product or its components and for the manufacturer to release patches to fix them. Updates also enable functionality changes, fix bugs not related to security, or otherwise improve the device's performance.

It is important that device updates are installed securely. It is particularly important that a device can verify that an update is from a legitimate source and hasn't been tampered with. If the update is not verified before it is installed, attackers may be able to exploit the update process to gain control of the device or weaken its security.

Guideline 1.1: The manufacturer shall publish the minimum period for which the device will receive security updates.

Guideline 1.2: The device shall verify that an update is from a trusted source and that it was not altered during transit.

Guideline 1.3: The device should use best-practice cryptography to support secure updates. (Guidance on best-practice cryptography can be found on the NCSC webpage)

Guideline 1.4: The manufacturer shall publish a policy defining the regularity and frequency of updates.

Guideline 1.5: Device updates shall be provided in response to critical vulnerabilities and incidents.

Guideline 1.6: Updates shall be manageable and flexible for administrators or other authorised entities (either users or other devices or services) across device fleets.

Guideline 1.7: Details of updates shall be published that state which publicly known vulnerabilities have been mitigated.

2. Support appropriate authentication

A device needs to be able to determine whether a user can access specific functionalities or carry out actions such as making configuration changes. To restrict access where required, users must be properly authenticated, including those with higher levels of privilege.

Not all authentication methods provide the same level of security. Stronger forms of authentication, such as hardware-backed technologies and multi-factor authentication, make it harder for an attacker to bypass defences, while pre-installed or default passwords provide no protection at all against an informed attacker.

Guideline 2.1: The device shall only grant access to a user following successful authentication.

Guideline 2.2: The device shall support authentication with other devices, services and networks. (*This guideline applies to all devices that can communicate sensitive or user data)*

Guideline 2.3: After initial setup, any credentials shall either be defined by the user or be unique to the device.

Guideline 2.4: Pre-installed credentials shall be generated using a mechanism that reduces the risk of automated attacks against a class or type of device. (*This guideline applies to devices that use pre-installed credentials that are unique per device)*

Guideline 2.5: All authentication protocols used on the device shall adhere to current best practice, such as using authentication protocols based on standardised technologies.

(Guidance on best practice can be found on the NCSC webpage)

Guideline 2.6: The device should support hardware-backed methods of authentication.

Guideline 2.7: Device identity should be bound to the physical device in a non-exportable fashion.

3. Protect data at rest and in transit

Data stored on a device and transmitted to and from it is often sensitive in nature. This may include data relating to its users, the enterprise, functionality or other information necessary for the device to operate securely.

It's important that data on the device is appropriately protected so an attacker can't read or modify it. Data transmitted to and from the device must also be appropriately protected, so it can not be stolen or tampered with. Throughout this principle, data is considered sensitive if its compromise could directly or indirectly cause financial, reputational or personal harm to its owner or anyone associated with it. Any device that holds such information is therefore also considered sensitive. This also includes security-relevant data and isn't limited to private keys, passwords and other credentials.

Guideline 3.1: The device should support the encryption of all user data at rest.

Guideline 3.2: When active, the device should support encryption of data. (*This guideline applies to all end user devices)*

Guideline 3.3: The device shall protect sensitive data in transit using a secure transport mechanism or application layer protocol that provides confidentiality, integrity and authenticity.

Guideline 3.4: The device shall use best-practice cryptography when protecting data at rest and in transit.

Guideline 3.5: Long-term cryptographic secret keys used for protecting data at rest or in transit shall be securely generated and stored.

Guideline 3.6: An authenticated and authorised user shall be able to delete sensitive data. *(This guideline applies to devices that are designed to store sensitive data)*

Guideline 3.7: Data should be compartmentalised, with appropriate access control.

4. Maintain device integrity

All devices rely on core software and firmware that are essential to their operation, such as their operating systems and bootloaders. If an attacker compromises or modifies this code, the attacker could control or subvert the device functionality. Compromised or modified code is challenging to identify and remove from the device.

Demonstrating that these crucial components are correct and have not been modified each time the device starts helps prevent the device booting into a pre-compromised state. This can be achieved by cryptographic checks based on a hardware root of trust, which make it substantially more difficult for an attacker to interfere.

Guideline 4.1: The firmware and operating system on the device shall only be modifiable using authorised update mechanisms.

Guideline 4.2: The device shall support pre-operating system boot security.

Guideline 4.3: The device should have a built-in framework for runtime integrity protection.

Guideline 4.4: The device shall provide documented exploit mitigation capabilities that shall be used by all system and pre-installed software.

Guideline 4.5: Integrity of device health data should be maintained on the device.

Guideline 4.6: The device can be physically hardened.

5. Ensure transparency of device health

Along with mechanisms to ensure device integrity, approaches such as zero trust rely on an organisation's services using a range of measurements to determine the health of a device. These measurements are often referred to as signals in zero trust deployments.

Technologies such as health attestation allow devices to provide these signals, as well as ensuring their cryptographic integrity.

When these signals are accessible to the organisation using the device (via their device management platform or other mechanisms), the organisation can make continuous risk assessments of the device to determine whether it remains in a trusted state.

Guideline 5.1: The manufacturer shall provide documentation of its definition of device health.

Guideline 5.2: During runtime, the health of the device shall be available locally.

Guideline 5.3: During runtime, the health of the device should be available remotely.

Guideline 5.4: The device should have a boot attestation process.

Guideline 5.5: The device should have a runtime attestation process that provides regular or continuous monitoring.

6. Permit only trusted software

If users can run untrusted software on a device, an organisation is likely to be exposed to malware threats such as ransomware. Depending on the device, both the manufacturer and the organisation need to have the capability to determine which software they trust. This software also includes the operating system and any software to support peripherals such as device drivers.

Mechanisms for determining and defining which software is trusted will often rely on cryptographic methods and by determining an allowed list of apps that users can install within a device management platform. Organisations may require different user roles to establish who is trusted to install and run software at different levels of trust.

Guideline 6.1: It shall be possible to restrict the use of software based on trust. *(This guideline applies to all devices that support the addition of non-pre-installed software (both first and third party))*

Guideline 6.2: Access to trusted tools shall be configurable per user by the organisation. *(This guideline applies to all devices that support configurations per user)*

Guideline 6.3: Restrictions on executing software should be configurable based on users or groups. (*This guideline applies to all devices where users' roles are configurable and where a device has the concept of an assigned user)*

7. Minimise the privilege and reach of applications

Minimising each application's privilege to a level that is only necessary for its function will minimise an attacker's access to privileges if the application is compromised. In addition, capabilities such as virtualisation and sandboxing further prevent an application from compromising the broader system. Escalating privilege is a typical goal for attackers, who often need elevated levels of control to gain persistence in a network and to achieve their goals. Minimising privileges across applications will make this step more difficult for attackers.

Guideline 7.1: The device shall limit application access to privacy-related features or peripherals until permission is granted by a user and/or administrator. *(Applies to devices where applications can be installed)*

Guideline 7.2: The device shall run software with the lowest permissions/privilege required for its operation. *(This guideline applies to all devices)*

Guideline 7.3: The device operating system should support a granular permissions model to enable the principle of least privilege.

Guideline 7.4: Software should be compartmentalised and prevented from interacting with other software and the system as a whole.

Guideline 7.5: The device should only be distributed with the software and hardware required for its functionality.

8. Constrain the use of all device interfaces

Interfaces, both logical and physical, are the gateways through which the device communicates with external entities. Interfaces have services which run over them; USB can provide both power and data, or a network interface can provide DNS and IP as services.

Ensuring devices only possess the interfaces necessary to operate, and appropriately validating use of interfaces, will restrict what an attacker can do. If a device has lots of open interfaces, whether network or physical, an attacker is more likely to discover a vulnerability to compromise the device. This is particularly true if unnecessary interfaces are available.

Guideline 8.1: It shall be made clear which services are running over both logical and external physical interfaces, and whether the user or organisation can disable those services.

Guideline 8.2: Users and organisations should be able to disable unnecessary services running over physical and logical interfaces.

Guideline 8.3: The device manufacturer shall provide a runtime mechanism to identify which services are exposed to the network and to document any known endpoints the device connects to.

Guideline 8.4: The manufacturer shall state which mitigations against interface misuse are available.

Guideline 8.5: Mitigations against interface misuse should be enabled by default.

Guideline 8.6: The device can provide the capability for interfaces to be disabled if not required.

9. Allow robust device management

Devices should be flexible in the way they are managed so that administrators can configure them to adhere to their organisation's security frameworks. For example, a corporately managed device will be managed differently to a Bring Your Own Device (BYOD). Whichever approach is taken, implementing effective device management ensures that crucial security features can't be modified or disabled by unauthorised users or malware.

Guideline 9.1: The device shall be configurable locally and via device management services.

Guideline 9.2: The administrator shall be able to enforce device configuration.

Guideline 9.3: The device should support automated enrolment and onboarding technologies.

Guideline 9.4: The device can use open standards and mechanisms for communicating with device management platforms.

Guideline 9.5: Configurations for the device should be exportable and importable as files.

10. Provide security logging, alerting and monitoring capabilities

It is important that devices can be monitored so administrators can identify potential security incidents, remove devices from the network (if necessary), or attempt to remediate any compromise.

The wide-ranging nature of cyber attacks means there is no single metric that can be used to identify a compromise in commodity attacks. Using antivirus techniques to identify known compromises will protect against some attacks for certain device types, but other data is necessary to identify novel attacks or misuse. This makes it important for a range of data to be made available through logging and monitoring systems, and for an alert system that can warn administrators of unusual behaviour on the device.

Guideline 10.1: The organisation shall be able to view security events related to the device, either locally or remotely.

Guideline 10.2: The device shall allow the organisation to apply indicators of compromise to network traffic.

*Indicators of compromise (IoCs) are used to identify the presence of malware, or a compromised device, in a network. If the device doesn't support the organisation in detecting IoCs in network traffic, compromise is likely to go unnoticed.

Guideline 10.3: The device shall support the capability to securely forward and export logs. (*This guideline applies to any devices capable of logging. This excludes constrained devices)*

Guideline 10.4: The device shall use reliable time sources to enable accurate security logging and investigation.

Guideline 10.5: The manufacturer shall provide documentation of formats for logs and events produced by the device. (*This guideline applies to any devices capable of logging. This excludes constrained devices)*

Guideline 10.6: Logging network connections enables an organisation to identify indicators of compromise.

- *(End user devices shall provide capabilities to log all network connections)*
- *(All other devices can provide capabilities to log all network connections*

Guideline 10.7: The device shall have the ability to alert the owner or administrator to significant changes in state.

11. <u>Enable recovery to a known good state</u>

Many devices will be compromised or infected at some point, but some users or organisations might be reluctant to dispose of an affected device, particularly if there is uncertainty about whether a compromise has occurred.

It's important that a device can be recovered into a known good state through a factory reset or another method to wipe all potentially harmful data from the device. Organisations won't then have to choose between using a potentially infected device and purchasing new devices in the event of a possible compromise.

Guideline 11.1: The device shall be capable of being reset into a 'known state'.

Guideline 11.2: It should be possible to remotely wipe the device.

Guideline 11.3: It should be possible to lock the device remotely through device management platforms. *(This guideline applies to all end user devices)*

Guideline 11.4: Linking data stored on the device with enterprise data repositories enables the backup and sync of data.

- *(Laptops, desktops and mobile devices shall have a mechanism for linking on-device user data storage with enterprise data repositories)*
- *(All other device types can have a mechanism for linking on-device user data storage with enterprise data repositories)*

Chapter 4: Proposed Interventions

We propose that a two-part approach to improving the cyber security of enterprise connected device security would be most effective. Subject to feedback, this approach will involve finalising and publishing the Code of Practice for Enterprise Connected Device Security and then taking steps to introduce either a voluntary pledge, developing an international standard, and/or developing new legislation, subject to Parliamentary approval. These interventions are set out below in more detail.

Based on the research, available at www.gov.uk/government/publications/research-on-cyber-security-in-enterprise-connected-devices , the current level of cyber security in some commonly used enterprise connected devices is low. Adherence to the principles in the proposed Code of Practice for Enterprise Connected Device Security would provide a baseline of protection against some common vulnerabilities. We are therefore seeking input to better understand if, or how, each intervention could support efforts to improve the security of enterprise connected devices from development to deployment and throughout their lifecycle. We are also asking for suggestions of new policy options, that would help improve the cyber security standard of enterprise connected devices.

Intervention 1: Creating a voluntary pledge

We propose creating a voluntary and non-legally binding pledge that manufacturers of enterprise connected devices could sign up to. The pledge would require signatories to publicly commit to showing measurable progress against some, or all, of the principles outlined in the Code of Practice for Enterprise Connected Device Security within a specified timeframe. The pledge will be published by DSIT, and signatories will therefore benefit from the greater public recognition of their commitment to improving the cyber security of their products. Signatories could be encouraged to provide transparency reports to provide purchasers with information about the security of their devices.

Industry should be at the forefront of pushing device security standards and creating innovative solutions to complex issues. This approach would allow organisations who are already taking important steps to develop and deploy enterprise connected devices more securely to highlight their strengths. Similarly, those that want to commit to doing more can do so by signing up to the pledge. A pledge would act as an incentive for manufacturers who seek to become market leaders and a trusted secure brand.

Intervention 2: Creating a new global standard

We propose the creation of a new global standard based on the Code of Practice for Enterprise Connected Device Security. Global standards are widely recognised by manufacturers and international governments as an effective way of establishing a baseline level of cyber security. Global standards, such as ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements) have been adopted globally and have helped to establish international consensus around what best practice looks like.

DSIT has commissioned work to map the existing international standards landscape for enterprise connected devices to the principles used in the Code of Practice for Enterprise Connected Device Security. This research found that the principles and guidelines outlined in the Code of Practice could be used to form the basis for a new global standard due to their alignment with several existing publications and other standards for connected devices. The

research concluded that whilst there were some similarities, none of the security requirements for consumer or industrial connected devices that were reviewed considered enterprise environments and the different threat landscape that comes with them.

Global standards for cyber security can help increase trust and confidence in a manufacturer's devices and provide coherent security protections across international markets. Our research and engagement have indicated that government could pursue the creation of a new global standard based on the Code of Practice for Enterprise Connected Device Security. Creation of a new standard for enterprise connected devices security would help improve security across several international markets.

The new global standard would not supplant the regulatory requirements for "consumer connectable products" or other international standards relating to IoT cyber security, including ETSI EN 303 645 and the draft ISO standard 27402. Instead, it seeks to build upon and align with other standards by setting security-related best practice for connected devices used in an enterprise setting.

Intervention 3: Legislation

Lastly, we may introduce legislation to enshrine some, or all, of the principles in the Code of Practice for Enterprise Connected Device Security into law. Given the global nature of supply chains, it can be difficult to influence the market to improve the cyber security of devices from the design stage and maintain security throughout a device's lifecycle. Mandating security by introducing legislation is often a last resort for the government but it can, in some cases, be the only way to promote the change required.

The PSTI Act 2022 brought about much needed protections to improve the security of consumer connected devices. One option available to government is updating the PSTI Act via primary legislation to broaden the scope of the regime to include both consumer and enterprise connected devices. Alternatively, another legislative vehicle could be used to do this if it is deemed more appropriate.

Unlike consumers, businesses have a greater capability to ensure that important security mitigations are in place, such as having dedicated staff to ensure that security updates are promptly rolled out to fix issues and a greater understanding of their network. We will therefore consider placing specific obligations on businesses and other end users to take specific actions.

We will publicly consult on all legislative plans, should we decide to pursue this intervention. As always, the introduction of any new legislation will be subject to Parliamentary approval.

Chapter 5: Next Steps and Future Policy Approach

This Call for Views will be live for eight weeks, from 12th May to 7th July. Stakeholders are invited to provide specific feedback via an online survey form on the proposed interventions, the proposed Code of Practice for Enterprise Connected Device Security and whether any additional interventions should be taken forward. Please see Annex A for the full Call for Views Survey Questionnaire.

We encourage stakeholders to provide any data that considers the financial and wider impacts associated with the implementation of the proposed interventions outlined in this document. All data will be treated confidentially, and participants will have the opportunity to identify themselves or choose to be anonymous when they submit their responses.

Responses can also be submitted to ecdsecurity@dsit.gov.uk, but we recommend that these are provided in the template that accompanies this publication. A downloadable copy of the template can be found [here]. If necessary, you can also submit written comments to the Call for Views on the Cyber Security of Enterprise Connected Devices, Critical Technologies Policy Team, Cyber Security & Digital Identity Directorate, Department for Science, Innovation & Technology, Level 3, 22 Whitehall, London, SW1A 2EG.

Further engagement will be undertaken in the coming months to seek feedback on the proposed interventions. DSIT also plans to arrange workshops with industry bodies, expert groups, and academics to help gather feedback.

Following the close of this Call for Views, we will review the feedback provided. We plan to publish a government response which provides an overview of the key themes from the Call for Views.

Annex A: Call for views survey questions

Section 1: Demographic questions

1. **Are you responding as an individual or on behalf of an organisation**? [drop-down menu, single choice]
    - Individual
    - Organisation
2. [If individual] **Which of the following statements best describes you?** [drop-down menu, single choice]
        - Cyber security professional
        - Consumer expert/advocate
        - Academic
        - IT professional
        - Interested member of the public
        - Other ['please specify' text box appears]

3. [If organisation] **Which of the following statements best describes your organisation?** [drop-down menu, single choice] (select all that apply)
    - manufacturer
    - IoT service or solution provider (businesses that help other businesses design, build, install and/or manage IoT systems)
    - Cyber security provider
    - Educational institution
    - Consumer group/organisation
    - Government
    - Retailer
    - Organisation that uses enterprise connected devices
    - Another actor in the enterprise IoT supply chain
    - Regulator
4. Other ['please specify' text box appears] [If manufacturer] **Which of the following statements best describes your organisation?** [drop-down menu, single choice]
    - The manufacturer of an entire enterprise connected device
    - The manufacturer of a device component

5. [If manufacturer] **What type of device, or device component, is made by your organisation?** [open-text – max 650 characters)

6. [if manufacturer] **Are your devices or device components used in an enterprise/ business setting?** [drop-down menu, single choice]
    - Yes
    - No
    - Don't know
7. [if no] Where and by whom are your devices or device components typically used? [open-text]

8. [If organisation] **What is the size of your organisation?** [drop-down menu, single choice]

- Independent or sole trader
- Micro (up to 9 employees and/or turnover under £2 million)
- Small (10-49 employees and/or turnover under £10 million)
- Medium (50-249 employees and/or turnover under £50 million)
- Large (250+ employees and/or turnover above £50 million)

9. [If individual], **Where are you based?** [drop-down menu, single choice]
    - England
    - Scotland
    - Wales
    - Northern Ireland
    - Europe (excluding England, Scotland, Wales and Northern Ireland)
    - North America
    - South America
    - Africa
    - Asia
    - Oceania
    - Other [please specify 'text box' appears]

10. [If organisation], **Where is your organisation headquartered?** [drop-down menu, single choice]
    - England
    - Scotland
    - Wales
    - Northern Ireland
    - Europe (excluding England, Scotland, Wales and Northern Ireland)
    - North America
    - South America
    - Africa
    - Asia
    - Oceania
    - Other [if selected, then a please specify text box appears]

11. [If organisation, and not headquartered in England, Scotland, Wales, Northern Ireland] **Does your organisation have a base in the UK?** [drop-down menu, single choice]
    - Yes/No
    - [If yes] please specify [open-text]

12. If you are happy for DSIT to contact you to discuss your response to this Call for Views and other work related to this policy development, please provide your email address. [open text]]
    -

Section 2: Questions on the Code of Practice for Enterprise Connected Device Manufacturers.

The following section contains questions about the 11 principles that would form the proposed Code of Practice, to allow you to provide feedback on each of the principles and their guidelines in turn. You will be able to give your views in detail on the set of proposed policy interventions in section 3 of this survey.

Principle 1: Provide updates, securely

- **Guideline 1.1:** The manufacturer shall publish the minimum period for which the device will receive security updates
- **Guideline 1.2:** The device shall verify that an update is from a trusted source and that it wasn't altered during transit
- **Guideline 1.3:** The device should use best-practice cryptography to support secure updates
- **Guideline 1.4:** The manufacturer shall publish a policy defining the regularity and frequency of updates
- **Guideline 1.5:** Device updates shall be provided in response to critical vulnerabilities and incidents
- **Guideline 1.6:** Updates shall be manageable and flexible for administrators or other authorised entities (either users or other devices or services) across device fleets
- **Guideline 1.7:** Details of updates shall be published that state which publicly known vulnerabilities have been mitigated

1. **Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?** [drop-down menu, single choice]

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Don't know

2. **Do you have any feedback on this principle? Yes/No [if yes]**[drop-down menu, open text box] Please provide your feedback in the relevant text box below.

Changes to Guideline 1.1		
Changes to Guideline 1.2		

Changes to Guideline 1.3		
Changes to Guideline 1.4		
Changes to Guideline 1.5		
Changes to Guideline 1.6		
Changes to Guideline 1.7		
Changes to the overall framing of the principle		
Suggestion of a new guideline		
Removal of principle		
Other feedback		

Principle 2: Support appropriate authentication

- **Guideline 2.1:** The device shall only grant access to a user following successful authentication
- **Guideline 2.2:** The device shall support authentication with other devices, services and networks
- **Guideline 2.3:** After initial setup, any credentials shall either be defined by the user or be unique to the device
- **Guideline 2.4:** Pre-installed credentials shall be generated using a mechanism that reduces the risk of automated attacks against a class or type of device
- **Guideline 2.5:** All authentication protocols used on the device shall adhere to current best practice
- **Guideline 2.6:** The device should support hardware-backed methods of authentication
- **Guideline 2.7:** Device identity should be bound to the physical device in a non-exportable fashion

3. **Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?** [drop-down menu, single choice]

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Don’t know

4. **Do you have any feedback on this principle? Yes/No [if yes] [drop-down menu, open text box]**

Changes to Guideline 2.1		
Changes to Guideline 2.2		
Changes to Guideline 2.3		
Changes to Guideline 2.4		
Changes to Guideline 2.5		
Changes to Guideline 2.6		
Changes to Guideline 2.7		
Changes to the overall framing of the principle		
Suggestion of a new guideline		
Removal of principle		
Other feedback		

Principle 3: Protect data at rest and in transit

- **Guideline 3.1:** The device should support the encryption of all user data at rest
- **Guideline 3.2:** When active, the device should support encryption of data
- **Guideline 3.3:** The device shall protect sensitive data in transit using a secure transport mechanism or application layer protocol that provides confidentiality, integrity and authenticity
- **Guideline 3.4:** The device shall use best-practice cryptography when protecting data at rest and in transit
- **Guideline 3.5:** Long-term cryptographic secret keys used for protecting data at rest or in transit shall be securely generated and stored
- **Guideline 3.6:** An authenticated and authorised user shall be able to delete sensitive data
- **Guideline 3.7:** Data should be compartmentalised, with appropriate access control

5. **Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?** [drop-down menu, single choice]
   - Strongly agree
   - Agree
   - Neither agree nor disagree
   - Disagree
   - Strongly disagree
   - Don't know

6. **Do you have any feedback on this principle? Yes/No [if yes]** [drop-down menu, open text box]

Changes to Guideline 3.1		
Changes to Guideline 3.2		
Changes to Guideline 3.3		
Changes to Guideline 3.4		
Changes to Guideline 3.5		
Changes to Guideline 3.6		
Changes to Guideline 3.7		
Changes to the overall framing of the principle		
Suggestion of a new guideline		
Removal of principle		
Other feedback		

Principle 4: Maintain device integrity

- **Guideline 4.1:** The firmware and operating system on the device shall only be modifiable using authorised update mechanisms
- **Guideline 4.2:** The device shall support pre-operating system boot security
- **Guideline 4.3:** The device should have a built-in framework for runtime integrity protection
- **Guideline 4.4:** The device shall provide documented exploit mitigation capabilities that shall be used by all system and pre-installed software
- **Guideline 4.5:** Integrity of device health data should be maintained on the device
- **Guideline 4.6:** The device can be physically hardened

7. **Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?** [drop-down menu, single choice]
   - Strongly agree
   - Agree
   - Neither agree nor disagree
   - Disagree
   - Strongly disagree
   - Don't know

8. **Do you have any feedback on this principle? Yes/No [if yes]** [drop-down menu, open text box]

Changes to Guideline 4.1		
Changes to Guideline 4.2		
Changes to Guideline 4.3		
Changes to Guideline 4.4		

Changes to Guideline 4.5		
Changes to Guideline 4.6		
Changes to the overall framing of the principle		
Suggestion of a new guideline		
Removal of principle		
Other feedback		

Principle 5: Ensure transparency of device health

- **Guideline 5.1:** The manufacturer shall provide documentation of its definition of device health
- **Guideline 5.2:** During runtime, the health of the device shall be available locally
- **Guideline 5.3:** During runtime, the health of the device should be available remotely
- **Guideline 5.4:** The device should have a boot attestation process
- **Guideline 5.5:** The device should have a runtime attestation process that provides regular or continuous monitoring.

9. **Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?** [drop-down menu, single choice]
   - Strongly agree
   - Agree
   - Neither agree nor disagree
   - Disagree
   - Strongly disagree
   - Don't know

10. **Do you have any feedback on this principle? Yes/No [if yes]** [drop-down menu, open text box]

Changes to Guideline 5.1		
Changes to Guideline 5.2		
Changes to Guideline 5.3		
Changes to Guideline 5.4		
Changes to Guideline 5.5		
Changes to the overall framing of the principle		
Suggestion of a new guideline		

Removal of principle		
Other feedback		

Principle 6: Permit only trusted software

- **Guideline 6.1:** It shall be possible to restrict the use of software based on trust
- **Guideline 6.2:** Access to trusted tools shall be configurable per user by the organisation
- **Guideline 6.3:** Restrictions on executing software should be configurable based on users or groups

11. **Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?** [drop-down menu, single choice]
- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Don't know

12. **Do you have any feedback on this principle? Yes/No [if yes]** [drop-down menu, open text box]

Changes to Guideline 6.1		
Changes to Guideline 6.2		
Changes to Guideline 6.3		
Changes to the overall framing of the principle		
Suggestion of a new guideline		
Removal of principle		
Other feedback		

Principle 7: Minimise the privilege and reach of applications

- **Guideline 7.1:** The device shall limit application access to privacy-related features or peripherals until permission is granted by a user and/or administrator
- **Guideline 7.2:** The device shall run software with the lowest permissions/privilege required for its operation
- **Guideline 7.3:** The device operating system should support a granular permissions model to enable the principle of least privilege

- **Guideline 7.4:** Software should be compartmentalised and prevented from interacting with other software and the system as a whole
- **Guideline 7.5:** The device should only be distributed with the software and hardware required for its functionality

13. **Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?** [drop-down menu, single choice]

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Don't know

14. **Do you have any feedback on this principle? Yes/No [if yes] [drop-down menu, open text box]**

Changes to Guideline 7.1		
Changes to Guideline 7.2		
Changes to Guideline 7.3		
Changes to Guideline 7.4		
Changes to Guideline 7.5		
Changes to the overall framing of the principle		
Suggestion of a new guideline		
Removal of principle		
Other feedback		

Principle 8: Constrain the use of all device interfaces

- **Guideline 8.1:** It shall be made clear which services are running over both logical and external physical interfaces, and whether the user or organisation can disable those services
- **Guideline 8.2:** Users and organisations should be able to disable unnecessary services running over physical and logical interfaces
- **Guideline 8.3:** The device manufacturer shall provide a runtime mechanism to identify which services are exposed to the network and to document any known endpoints the device connects to
- **Guideline 8.4:** The manufacturer shall state which mitigations against interface misuse are available
- **Guideline 8.5:** Mitigations against interface misuse should be enabled by default

- **Guideline 8.6:** The device can provide the capability for interfaces to be disabled if not required

15. **Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?** [drop-down menu, single choice]

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Don't know

16. **Do you have any feedback on this principle? Yes/No [if yes]** [drop-down menu, open text box]

Changes to Guideline 8.1		
Changes to Guideline 8.2		
Changes to Guideline 8.3		
Changes to Guideline 8.4		
Changes to Guideline 8.5		
Changes to Guideline 8.6		
Changes to the overall framing of the principle		
Suggestion of a new guideline		
Removal of principle		
Other feedback		

Principle 9: Allow robust device management

- **Guideline 9.1:** The device shall be configurable locally and via device management services
- **Guideline 9.2:** The administrator shall be able to enforce device configuration
- **Guideline 9.3:** The device should support automated enrolment and onboarding technologies
- **Guideline 9.4:** The device can use open standards and mechanisms for communicating with device management platforms
- **Guideline 9.5:** Configurations for the device should be exportable and importable as files

17. **Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?** [drop-down menu, single choice]
    - Strongly agree
    - Agree
    - Neither agree nor disagree
    - Disagree
    - Strongly disagree
    - Don't know

18. **Do you have any feedback on this principle? Yes/No [if yes]** [drop-down menu, open text box]

Changes to Guideline 9.1		
Changes to Guideline 9.2		
Changes to Guideline 9.3		
Changes to Guideline 9.4		
Changes to Guideline 9.5		
Changes to the overall framing of the principle		
Suggestion of a new guideline		
Removal of principle		
Other feedback		

Principle 10: Provide security logging, alerting and monitoring capabilities

- **Guideline 10.1:** The organisation shall be able to view security events related to the device, either locally or remotely
- **Guideline 10.2:** The device shall allow the organisation to apply indicators of compromise to network traffic
- **Guideline 10.3:** The device shall support the capability to securely forward and export logs
- **Guideline 10.4:** The device shall use reliable time sources to enable accurate security logging and investigation
- **Guideline 10.5:** The manufacturer shall provide documentation of formats for logs and events produced by the device
- **Guideline 10.6:** Logging network connections enables an organisation to identify indicators of compromise
- **Guideline 10.7:** The device shall have the ability to alert the owner or administrator to significant changes in state

19. **Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?** [drop-down menu, single choice]
    - Strongly agree
    - Agree
    - Neither agree nor disagree
    - Disagree
    - Strongly disagree
    - Don't know

20. **Do you have any feedback on this principle? Yes/No [if yes]** [drop-down menu, open text box]

Changes to Guideline 10.1		
Changes to Guideline 10.2		
Changes to Guideline 10.3		
Changes to Guideline 10.4		
Changes to Guideline 10.5		
Changes to Guideline 10.6		
Changes to Guideline 10.7		
Changes to the overall framing of the principle		
Suggestion of a new guideline		
Removal of principle		
Other feedback		

Principle 11: Enable recovery to a known good state

- **Guideline 11.1:** The device shall be capable of being reset into a 'known state'
- **Guideline 11.2:** It should be possible to remotely wipe the device
- **Guideline 11.3:** It should be possible to lock the device remotely through device management platforms
- **Guideline 11.4:** Linking data stored on the device with enterprise data repositories enables the backup and sync of data

21. **Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?** [drop-down menu, single choice]
    - Strongly agree
    - Agree
    - Neither agree nor disagree

- Disagree
- Strongly disagree
- Don't know

22. **Do you have any feedback on this principle? Yes/No [if yes]** [drop-down menu, open text box]

Changes to Guideline 11.1		
Changes to Guideline 11.2		
Changes to Guideline 11.3		
Changes to Guideline 11.4		
Changes to the overall framing of the principle		
Suggestion of a new guideline		
Removal of principle		
Other feedback		

23. **Are there any other broad principles you feel should be included in the current version of the proposed Code of Practice for Enterprise Connected Device Security?** [drop-down menu, single choice]

- Yes/No
- [If yes], please specify what principle you would like to be included and why [open-text]

Section 3: Questions about our policy approach.

In this section we would like to get your views on each of the policy options proposed in the Call for Views document. Your opinions

and feedback will help shape the Government's approach to securing enterprise connected devices.

24. **Do you agree or disagree with the following statement: There is a need for government to do more to encourage greater cyber security in enterprise connected devices.** [drop-down menu, single choice]
    - Strongly agree
    - Agree
    - Neither agree nor disagree
    - Disagree
    - Strongly disagree
    - Don't know

    Please specify why.

25. **Do you agree or disagree with the following statement: The cyber risks posed to enterprise connected devices are sufficiently different to other IoT devices to warrant an independent code of practice.** [drop-down menu, single choice]
    - Strongly agree
    - Agree
    - Neither agree nor disagree
    - Disagree
    - Strongly disagree
    - Don't know

    Please specify why

26. **[**if manufacturer or service/solution provider (Q3)] **Would your organisation face any practical challenges in implementing the principles outlined in the Code of Practice? [drop-down menu, single choice]**
    - **Yes/No/Don't know**
    - **[If yes] Please specify [open text]**

The next section of questions will ask for your views on the interventions outlined in chapter 3 of the Call for Views.

Option 1: Voluntary pledge

This option proposes that the proposed Code of Practice for Enterprise Connected Device Security forms the basis of a voluntary pledge that would help organisations commit to their products achieving a baseline of cyber security over a set period.

27. **Would you agree with implementing this measure?** [drop-down menu, single choice]

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Don't know

Please specify why [open-text]

28. [If manufacturer or IoT service/solution provider (Q3)] **Would your organisation sign up for a voluntary pledge?**
    - **Yes/No/Don't know**

    Please specify why [open-text]

Option 2: Creating a new global standard.

This option proposes that the proposed Code of Practice for Enterprise Connected Device Security forms the basis of a new global standard, through the standardisation organisation ETSI.

29. **Would you agree with implementing this measure?** [drop-down menu, single choice]
- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Don't know
- **Please specify why** [open-text]

Option 3: Legislation.

This option proposes that government mandates a standard of cyber security in enterprise connected devices.

30. **Would you agree with creating new legislation that creates legal obligations for enterprise connected device manufacturers?** [drop-down menu, single choice]
- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Don't know

Please specify why [open-text]

31. **Would you agree with broadening the scope of the consumer IoT legislation (Product Security and Telecommunications Infrastructure Act 2022) to cover enterprise connected products?** [drop-down menu, single choice]
- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- Don't know
- **Please specify why** [open-text]

32. **Please rank the following interventions in order of preference.**
Drag and drop the options into your chosen order.
    - Creating a voluntary pledge.
    - Creating a new global standard.

- Broadening the scope of the existing consumer IoT legislation (PSTI Act 2022).
- Introducing new legislation that creates legal obligations for enterprise connected device manufacturers.

33. **Are there any other interventions that the government should consider that would help improve the security of enterprise connected devices.** [drop-down menu, single choice]

- Yes/No
- [If yes], please specify what intervention and why [open-text]

Thank you for taking the time to complete this survey and provide your feedback on the outlined policy approach. .