# Annex A: Call for views survey questions

## Section 1: Demographic questions

1. Are you responding as an individual or on behalf of an organisation?

Organisation

1. Which of the following statements best describes your organisation?

Other: Association

1. What is the size of your organisation?

250

1. Where is your organisation headquartered?

England

1. 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.

john.moor@iotsecurityfoundation.org

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

### Principle 1: Provide updates, securely

1. Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?

Strongly agree

1. Do you have any feedback on this principle?

Yes

|  |  |  |
| --- | --- | --- |
| Changes to Guideline 1.1 |  |  |
| Changes to Guideline 1.2 | x | Security updates should be digitally signed in accordance with the EV Code Signing Certificate guidelines by the CA/Browser Forum |
| 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 | x | It should also be noted more clearly that to provide a secure update then section 4 Maintain Device Integrity (and 5.4) is vital such that a securely implemented Root of Trust forms the basis of the chain of trust needed to reach the point where a device update can be performed |

### Principle 2: Support appropriate authentication

1. Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?

Strongly agree

1. Do you have any feedback on this principle?

Yes

|  |  |  |
| --- | --- | --- |
| 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 | x | any form of MFA should be sufficient (i.e., various authenticator apps, OTPs, etc.) |
| Changes to Guideline 2.7 |  |  |
| Changes to the overall framing of the principle |  |  |
| Suggestion of a new guideline |  |  |
| Removal of principle |  |  |
| Other feedback | x | * Agreed some form MFA should be performed where possible. BUT, allow for this needing to be an automatic, interface and user interaction free process for connected embedded devices since many will be on the network with no user interface or intervention. Capabilities exist to achieve this but the wording may be coming from an IT perspective.
* Consider here the work being done on the NIST Trusted Onboarding that the new IoTSF Working Group are working on. This will go a long way to providing mutual trust.
* The requirements also seem biased toward there being some form of user logging into a device and hence a UI which may not exist on many connected devices. BUT, devices which default to a least privilege state is good.
* To meet some of the later requirements for devices to be capable of being locked out over the network, which assumes it can be connected with via a more privileged account should also spell out that unique ‘administrator’ level credentials per device shall be enforced to limit scope of a single set of credentials being able to access multiple devices. This will help with individual access to devices directly from the network where limited logging exists on the end device. Where a central management interface is used then individual credentials should be maintained but the management software should then have sufficient logging, account protection and misuse detection implemented to spot an malicious attempt to use the management interface to access all devices.
 |

### Principle 3: Protect data at rest and in transit

1. Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?

Strongly agree

1. Do you have any feedback on this principle?

Yes

|  |  |  |
| --- | --- | --- |
| 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

1. Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?

Neither agree nor disagree

1. Do you have any feedback on this principle?

Yes

|  |  |  |
| --- | --- | --- |
| 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 | x | 4.7 Disable debug interfaces on the hardware4.8 Provide evidence of the secure provisioning of the Root of Trust such that integrity in the manufacturing process, creation and initial deployment of keys and device secrets plus the operational management of keys and key rotation mechanisms maintain overall system integrity |
| Removal of principle |  |  |
| Other feedback | x | Many of the requirements noted are rooted in the capabilities of IT devices running on complex platforms using a ‘big iron’ OS such as Windows or Linux. Many of the ideas around network management of devices, whilst a good idea in themselves, from an IT operations perspective, can be difficult to implement on cost and resource constrained devices that would be used in a ‘connected device’. Many of the requirements within this call for views are echoed with CRA also and pose a significant challenge. They will require a large amount of change to ‘connected devices’ as the hardware used on many of them to meet the cost constraints imposed by purchasers DO NOT have the physical resources or the enterprise grade operating system available for them. To implement such enterprise grade features in cost and resource constrained devices will result in many devices needing to be wholly re-designed with appropriate forward looking components and utilsing operating system features, many of which don’t exist for these devices yet. This ultimately will increase product cost. |

### Principle 5: Ensure transparency of device health

1. Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?

Agree

1. Do you have any feedback on this principle?

Yes

|  |  |  |
| --- | --- | --- |
| Changes to Guideline 5.1 |  |  |
| Changes to Guideline 5.2 | x | may be tricky to implement if not UI. Sure can add LED’s and have flashing signals on them but you have to be able to interpret the LED. So this requirement may be limited in what it can achieve. |
| 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 | x | 5.6 The manufacturer shall provide documentation on the SBOM of the software running on the device5.7 The manufacturer should provide attestation about the development process |
| Removal of principle |  |  |
| Other feedback |  |  |

### Principle 6: Permit only trusted software

1. Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?

Stringly agree

1. Do you have any feedback on this principle?

Yes

|  |  |  |
| --- | --- | --- |
| Changes to Guideline 6.1 | x | It should only be allowed to run digitally signed and trusted applications |
| Changes to Guideline 6.2 |  |  |
| Changes to Guideline 6.3 |  |  |
| Changes to the overall framing of the principle |  |  |
| Suggestion of a new guideline | x | Provide proof of integrity of secure development process and method by which updates are created and signed. Secure Software Supply Chain and NIST SLSA is a good starting point for this. |
| Removal of principle |  |  |
| Other feedback |  |  |

### Principle 7: Minimise the privilege and reach of applications

1. Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?

Agree

1. Do you have any feedback on this principle?

Yes

|  |  |  |
| --- | --- | --- |
| 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 | x | Principle of Least Privilege is great but some of these requirements are again assuming a PC/Linux level of capability. Compartmentalisation on constrained devices is not impossible BUT isn’t generally available today…..though it arguably should be. So a lofty goal that will take several years to achieve. However, a constrained device should also only be running one application and wouldn’t normally have supplementary apps loadable by the user. It should be working at the single device image level of functionality. |

### Principle 8: Constrain the use of all device interfaces

1. Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?

Strongly agree

1. Do you have any feedback on this principle?

Yes

|  |  |  |
| --- | --- | --- |
| 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 | x | 8.7 Devices shall be delivered in the most secure default configuration8.8 Devices shall minimize attack surface8.9 Manufacturers shall document all interfaces (physical, network, wireless)8.10 Physical Debug/Programming ports shall be disabled8.11 Ports which provide debug logging information shall be disabled.8.12 To limit potential attack surfaces only those protocols that a device needs to perform it’s functions shall be available on the device. This should limit building all protocols just in case and disabling them. Being disabled but loaded and available makes an attackers job easier via exploiting a bug in a disabled protocol or through EoP allowing an idle protocol to be enabled and misused.8.13 Ideally firewalls should have rules to match the enabled protocols and limit scope for misuse of a disabled protocol. As a secondary level of defence. |
| Removal of principle |  |  |
| Other feedback |  |  |

### Principle 9: Allow robust device management

1. Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?

Strongly agree

1. Do you have any feedback on this principle?

Yes

|  |  |  |
| --- | --- | --- |
| 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 | x | may prove tricky on constrained devices as assumes a file system and file storage mechanism exist. Maybe modify to cover mechanism such as SNMP or provision of a XML, MQTT data etc. |
| 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

1. Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?

Strongly agree

1. Do you have any feedback on this principle?

Yes

|  |  |  |
| --- | --- | --- |
| 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 | x | 10.8 Devices shall assure that no secrets or personal / sensitive information ends up in log files |
| Removal of principle |  |  |
| Other feedback | x | - Agree in principle BUT allow for constrained devices having limited storage on which to write a log. This will normally be shared with the secure update image store which will likely also contain the default recovery image and may be the last known good image so space for logging data may be restricted to the kB’s range. Note also that erase/write limitations on flash memory storage could soon be exceeded if too much data is regularly written and erased.- Again, depending how the log files are presented across the network e.g. if it is expected to be in a Windows/Linux compatible file format or available as a network drive severely impacts the code size and increases the attack surface and vulnerability potential of a constrained device. Allowing secure local storage to minimise tampering potential and provision of log in a web friendly format that can be sent to the connected device management interface may achieve the same overall effect but with consideration for the device constraints. |

### Principle 11: Enable recovery to a known good state

1. Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?

Strongly agree

1. Do you have any feedback on this principle?

Yes

|  |  |  |
| --- | --- | --- |
| Changes to Guideline 11.1 | x | Suggest extending this to say a ‘known secure state’ which implies that all PII or sensitive data is securely erased. |
| Changes to Guideline 11.2 |  |  |
| Changes to Guideline 11.3 |  |  |
| Changes to Guideline 11.4 |  | similar problem as in 10 above. Having a method that links files on the device that is compatible with broad compatibility errs towards files and filesystems with the knock-on effect on capabilities and resources. If the mechanism allows for provision of data via the device management software and creation / sharing of data indirectly via the device management interface this helps reduce the burden on the constrained device. |
| Changes to the overall framing of the principle |  |  |
| Suggestion of a new guideline |  | 11.5 To prevent device rollback in the event of a failed update or detection of malicious event, tempering etc. The device shall recover to a default secure state using a recovery or sandbox image that will ensure all sensitive data or network settings are securely erased and the device shall re-perform the provisioning process. The provisioning process would require connection to an isolated sandbox to allow secure device recovery to be performed and relevant checks to ensure checks for malicious activity and removal or isolating of the previous device entry in the management software. |
| Removal of principle |  |  |
| Other feedback |  |  |

## Section 3: Questions about our policy approach.

1. 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.

Strongly agree

While voluntary adherence to security requirements is ideal, history has shown that without legislative mandates, progress is slow. Therefore, introducing legislation, or at the very least, a certifiable standard verified by enterprise consumers, is necessary to drive industry-wide compliance.

1. 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.

Disagree

Creating sector-specific legislation or codes of practice may lead to further fragmentation. A more unified approach, akin to the CRA, where all connected products are in scope unless specifically exempted, would be more effective. This approach acknowledges that while IT, OT, enterprise, and industrial networks have differences, they share common vulnerabilities and attack vectors. A unified set of product requirements would simplify compliance and reduce administrative burdens.

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

1. Would you agree with implementing this measure?

Strongly disagree

While the intention behind a voluntary pledge is commendable, the history of cybersecurity across industries has shown that voluntary measures alone are insufficient to bring about the necessary change. Many organisations will delay action until compelled by regulation or enforcement. Without legal accountability or market consequences, such as enforced certification or penalties for non-compliance, a voluntary pledge risks becoming a symbolic gesture with limited real-world impact.

Experience with frameworks like the Product Security and Telecommunications Infrastructure (PSTI) Act has shown that even when legislation exists, awareness and adherence can lag unless there are clear enforcement mechanisms and consequences. A voluntary pledge may help raise awareness but should not be relied upon as the primary or only intervention.

Option 2: Creating a new global standard.

1. Would you agree with implementing this measure?

Neither agree nor disagree

Creating a new global standard via ETSI could provide long-term value, especially if it builds on existing initiatives and aligns with international efforts like the EU Cyber Resilience Act (CRA). However, care must be taken to avoid contributing to further fragmentation. There are already several relevant standards in this space (e.g., ETSI EN 303 645, IEC 62443, NIST frameworks), and introducing yet another could increase the burden on manufacturers - particularly those with limited resources - by forcing them to comply with multiple overlapping requirements depending on geography or sector.

Instead, this effort should aim to **harmonise** with existing global standards, not duplicate or diverge from them. The ideal outcome would be to unify security expectations across sectors (IT, OT, IoT) and geographies, thereby reducing complexity and compliance costs while improving overall security posture. If implemented carefully and in coordination with other major frameworks, this option could significantly improve consistency and clarity in enterprise device security.

Option 3: Legislation

1. Would you agree with creating new legislation that creates legal obligations for enterprise connected device manufacturers?

Strongly agree

Voluntary efforts and pledges have consistently fallen short in driving meaningful, industry-wide cybersecurity improvements. Legislation is necessary to establish a clear, enforceable baseline for enterprise connected device security. Without legal obligations, many manufacturers - especially those under commercial pressure - are unlikely to prioritise security, leaving enterprise environments exposed to preventable risks.

However, for legislation to be effective, it must include:

* Clear and enforceable requirements, preferably harmonised with existing standards (e.g. CRA, IEC 62443, NIST);
* Mechanisms for compliance verification (e.g. certification or conformity assessment);
* Provisions for enforcement and penalties, not just guidance;
* Consideration for constrained devices where full compliance may be technically challenging, offering tailored expectations without weakening the baseline.

Legislation backed by effective enforcement is the most viable path to raising the security bar across the industry and protecting critical enterprise environments from increasing cyber threats.

1. Would you agree with broadening the scope of the consumer IoT legislation (Product Security and Telecommunications Infrastructure Act 2022) to cover enterprise connected products?

Strongly agree

Broadening the PSTI Act to include enterprise connected products would create a more unified and efficient regulatory framework. Many of the risks faced by consumer and enterprise connected devices are similar, especially as the boundary between consumer and enterprise devices continues to blur. A unified approach would reduce fragmentation, avoid duplication of effort, and help address the significant skills gap in cybersecurity by simplifying compliance requirements. It would also allow for faster implementation compared to building an entirely new legislative framework from scratch.

1. Please rank the following interventions in order of preference.
	1. Broadening the scope of the existing consumer IoT legislation (PSTI Act 2022)
	2. Introducing new legislation that creates legal obligations for enterprise connected device manufacturers
	3. Creating a new global standard
	4. Creating a voluntary pledge
2. Are there any other interventions that the government should consider that would help improve the security of enterprise connected devices

Yes

The government should consider establishing a certification and labelling scheme that allows enterprise consumers to easily verify a device's security posture. This could be aligned with international efforts like the EU CRA or US NIST labeling initiatives. Certifications should be based on measurable, testable criteria and tied to security assurance levels, helping procurement teams make informed choices and incentivising manufacturers to meet higher standards.

Additionally, funding support or tax incentives for SMEs to comply with new security standards would help mitigate the cost burden and encourage broader adoption across the supply chain.