PUBLIC CONSULTATION ON:

Internet of Things (IoT) Security Standard

14 November 2021

Part 1: General Information

Legal Disclaimer

This Consultation is not a binding legal document and also does not contain legal, commercial, financial, technical or other advice. The Telecommunications Regulatory Authority is not bound by it, nor does it necessarily set out the Authority's final or definitive position on particular matters.

Invitation to Public Consultation

Request for comments

1. The Telecommunications Regulatory Authority (the "Authority") invites all interested parties to submit written comments with regard to the issues addressed in the consultation document.

2. The Authority particularly welcomes comments and responses to the specific numbered questions set out in the "Public Consultation on Internet of Things (IoT) Security Standard" supported by appropriate substantiation.

3. Responses should be sent to the Authority preferably by email (PDF format) or post (Comments submitted in printed format, especially by post, must be accompanied by a CD-ROM or USB storage key containing the same comments in electronic format) to the attention of:

Telecommunications Regulatory Authority
P.O. Box: 3555
PC: 111, Seeb
Sultanate of Oman

Email: traoman@tra.gov.om

4. Responses should include:

   a. The name of the company/institution/association etc.;

   b. The name of the principal contact person;

   c. Full contact details (physical address, telephone number and e-mail address); and

   d. In the case of responses from individual consumers, name and contact details.

Format of comments

1. In providing their comments, interested parties are kindly requested to use the following template. In particular, any comment should clearly specify the numbered questions it is referring to and indicate any attachment relevant to the specific comment.

[Name of the company/ institution/ association]	{Name of principal contact person, and position}	[Contact information i.e. email address, telephone number, fax number, postal address etc.]
[Enter number of question] Example: Q1	[Enter here the exact wording of the question referred to]	
Comment	[Enter here your comment on the question referred to above]	
Substantiation	[Enter here the substantiation in support of your comment]	
Attachment	[Enter here number and title of any attached document relevant to your comment]	

2. The Authority expects the comments to follow the same order as the one set in the “Public Consultation on Internet of Things (IoT) Security Standard” and summarized in the list of questions.

3. The Authority also invites respondents to substantiate their responses. Any response submitted without any substantiation may not be considered. In case of disagreement with one of the approaches proposed by the Authority, the respondent is invited to provide an alternative to such approach together with detailed justifications.

4. In the interest of transparency, the Authority intends to make all submissions received, available to the public. The Authority will evaluate a request for confidentiality in line with relevant legal provisions.

5. Respondents are required to mark clearly any information included in their submission that is considered confidential. Where such confidential information is included, respondents are required to provide both a confidential and a non-confidential version of their submission (soft copies and not scanned copies). If a part or a whole submission is marked confidential, reasons should be provided. The Authority may publish or refrain from publishing any document or submission at its sole discretion.

Way Forward

1. This consultation is open for public comments.
2. All relevant (substantiated) comments will be reviewed and the Authority may, at its sole discretion, consider those acceptable. Therefore, the Authority will not be bound to comply with any comment or opinion received and may not respond to comments or opinions individually or more clarification concerning this specific consultation process, interested parties are invited to contact.

Part 2: The Consultation

Public Consultation on IoT Security Standard

Preamble

The Internet of Things (IoT) environment consists of a network of various connected stationary and mobile devices which can interact with the physical environment surrounding them. These connections are enabled by a number of supporting technologies including sensing, networking, and information technologies among others.

There are various use cases of IoT technologies and many industries, governments, as well as consumers enjoy many benefits from IoT technologies such as convenience, efficiency in workflows and cost-cutting. While IoT provides significant benefits for a wide range of stakeholders, IoT devices and systems also have certain vulnerabilities which may be exploited by threat agents, making them easy targets for cyber-attacks. Given the importance of IoT technologies to the creation of a digital society in the Sultanate, it follows that security of IoT is of utmost importance for all stakeholders within the value chain.

As part of TRA's mandate towards embracing new technologies and services in the Sultanate, TRA is continuing the work it started to formulate an appropriate regulatory position that will support further uptake of IoT services in the Sultanate while ensuring their security. TRA's approach towards formulating this position is based on the existing international development and experience while taking into consideration the legal and regulatory frameworks in the Sultanate.

After its drafting of the IoT Security Standard for the Sultanate, TRA is proceeding with this public consultation in order to understand the views of relevant stakeholders on the overall approach and controls outlined in the Standard.

Definitions of key concepts

- IoT Security Standard: Refers to a document including a set of security requirements and technical measures aimed at various relevant stakeholders responsible for ensuring the security of end-to-end IoT solutions
- Security domain: Refers to the grouping of security requirements and technical measures per topic
- Security control / sub-control: Refers to the security requirements and technical measures aimed at various stakeholders responsible for ensuring the security of end-to-end IoT solutions

IoT Security Standard

Article (1): In the application of the provisions of this Standard, the following words and expressions shall have the meaning assigned against each:

a. **Internet of Things (IoT) services**: Services provided via a system to manage, operate and monitor IoT devices and M2M communication devices as a whole or in part, and to send, receive and analyze data and information by linking this system to the licensed communications networks in the Sultanate.

b. **Vendor**: Providers of IoT-related hardware and software both for the back end and user side.

c. **IoT service provider**: Specialized companies that develop and offer only IoT services.

d. **Integrator:** Companies that act ask the middleman between IoT services and devices by integrating such components to client networks / systems.

e. **Licensee:** Any telecommunication service provider in Oman holding a Class 1, 2, or 3 license from TRA.

Article (2): The controls outlined in this Standard are appliable to **vendors, IoT service providers, integrators, and licensees** in the Sultanate of Oman. In each case, the Standard defines the intended outcome of the implementation of the controls but does not give direction on how the implementation itself should be done, as this is left to the discretion of the stakeholders.

Article (3): With respect to the **Mandatory IoT Security Controls,** the TRA withholds the right to apply compliance checks through audits, third-party assessments, imposed self-assessments, or any other means.

Article (4): A further set of **Voluntary IoT Security Controls** is provided that act as guidelines for applicable stakeholders but are not legally binding. However, in the interest of security within the sector, TRA strongly encourages stakeholders to review such controls and make serious efforts to implement them within a reasonable timeframe.

Article (5): Considering the rapidly evolving nature of IoT technologies, this Standard will be reviewed periodically by the TRA and, if deemed necessary, will be updated accordingly.

Article (6): This IoT Security Standard consists of 6 security domains, 11 security controls and 2 security sub-controls as Mandatory; and 13 security domains, 43 security controls and 8 security sub-controls as Voluntary.

Article (7): The control and subcontrol codes are assigned based on the applicability category and domain the controls belong to. The applicability categories are denoted as "M" for mandatory controls and subcontrols, and "V" as voluntary controls and subcontrols. The figure below illustrates this notation.

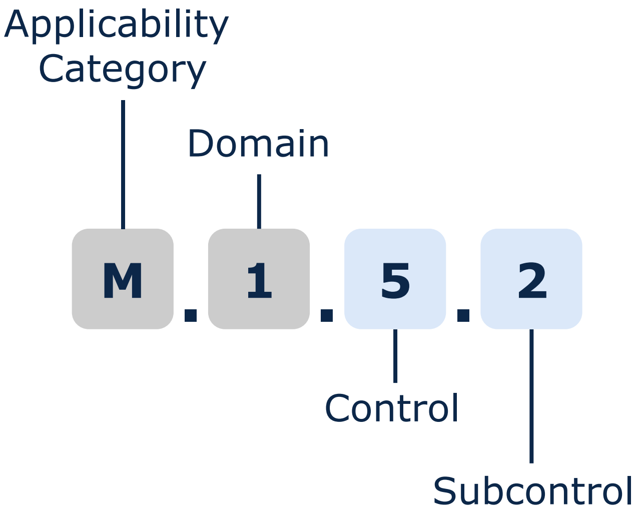

Figure 1. Control code notation structure

Article (8): The controls and subcontrols outlined in this document are presented following the structure below.

Applicability category & Domain number	**Domain name**	
Controls		Applies to
Control number	Control / subcontrol clause/s	Applicable stakeholder/s

Figure 2. Overview of controls per applicability category and domain

Article (9): All applicable stakeholders shall comply with the corresponding Mandatory IoT Security Controls outlined below.

M.1	**Cryptography**	
Controls		Applies to
M.1.1	M.1.1.1 - Default passwords shall be avoided. All the passwords used in the system, including users' passwords, shall have a minimum length, and should include lower-case letters, capital letters, numbers, and symbols. When generating passwords through an automatic function, approved algorithms must be used.	Vendors, Service Providers, Licensees
	M.1.1.2 - Developers shall avoid embedded credentials in device software or hardware. Storage of passwords should never be done using plain text; they must be hashed or encrypted, and they should have an expiry.	Vendors, Service Providers
M.2	**Data storage / protection**	
Controls		Applies to
M.2.1	Industry-proven transport protocols (e.g., OWASP, FIPS) shall be used with security controls that are properly activated and configured, granting that data is protected during transit. Personal data must also be encrypted (and anonymized, where possible) in transit and at rest.	Vendors, Service Providers, Integrators, Licensees
M.3	**Policy / governance**	
Controls		Applies to
M.3.1	Users should be assisted in assuring that the data processing operations of their products are functioning as specified, including clear guidance on how to secure privacy settings without losing device functionality, for example via device manuals or websites. Users must be informed about what private data is required for the device to function properly.	Vendors, Service Providers, Integrators
M.3.2	Consumers should be informed about the end-of-life policy of their products. This should include the minimum length of time in which a device will receive software updates and the consequences of not receiving updates. Also, users should be assisted in all stages of the cycle of life of the product, including installation, connection, operation and maintenance.	Vendors, Service Providers

M.4	**Privacy**	
Controls		Applies to
M.4.1	All stakeholders must adhere to Oman's Data Protection Laws and Regulations when developing, delivering, and processing data, granting that personal data is only accessible to authorized entities.	Vendors, Service Providers, Integrators, Licensees
M.4.2	Vendors and Service Providers must provide users with a mechanism to reset the device to a "factory default" state, for example a "wipe" button. This should include clear instructions on how to use it. The mechanism must grant that all the personal data stored in the device and in any associated backed can be deleted by users.	Vendors, Service Providers
M.4.3	Users' personal data shall only be shared with third parties after the users' consent is given. Sale or transfer of any identifiable user data should not take place unless it is a dependent part of the sale or liquidation of the core business.	Vendors, Service Providers, Licensees
M.4.4	Personal data should only be collected if necessary for the operation of the device. Devices' privacy settings should be privacy-protective by default. In addition to this, device manufacturers and IoT service providers must provide consumers with clear and transparent information about how their data is used, by whom and/or if the data is stored in any foreign country.	Vendors, Service Providers, Integrators, Licensees
M.5	**System security**	
Controls		Applies to
M.5.1	Vendors and service providers should not unnecessarily expose access to the system. This includes closing unrequired ports and interfaces, the ability to disable any network interface not necessary for the functionality of the device, and the possibility to restrict access to authorized entities only. Providers must not implement or use any backdoor or embedded credentials to gain remote access to the device.	Vendors, Service Providers
M.6	**Vulnerability management**	
Controls		Applies to

M.6.1	Disclosed vulnerabilities should be acted on in a timely manner. This includes but is not limited to; the provision of a public point of contact to report vulnerabilities, calling attention to the general users of the vulnerable application or device, and remediating the vulnerability without user intervention, where possible. When user intervention is required, users must be provided with clear, free, and easy-to-apply instructions.	Vendors, Service Providers
M.6.2	Regular penetration testing, threat modelling and monitoring should be performed to maintain awareness of vulnerabilities and maintain continuous improvement.	Service Providers

Article (10): All applicable stakeholders are strongly encouraged to comply with the corresponding Voluntary IoT Security Controls outlined below.

V.1	**Access management**	
Controls		Applies to
V.1.1	User authentication on the device or backend application should be provided in a secure way. User credentials should therefore be reinforced with multi-factor authentication whenever possible, especially for critical functions e.g., password reset.	Vendors, Service Providers
V.1.2	V.1.2.1 - For each IoT system or service, authentication functions that ensure the security of the entire IoT system or service should be applied.	Vendors, Service Providers
	V.1.2.2 - A suitable authentication method should be chosen considering the constraints on the functions and performance of the IoT devices.	Vendors, Service Providers
V.2	**Configuration management**	
Controls		Applies to
V.2.1	Secure default settings should be made when implementing or connecting IoT systems and services.	Vendors, Service Providers
V.3	**Data storage / protection**	
Controls		Applies to

V.3.1	Authentication and integrity protection should be applied to data.	Vendors, Service Providers
V.3.2	Functions should be considered that prevent records from being illegally deleted or falsified, for example setting log-access, authorization, and encryption for IoT devices and systems.	Vendors, Service Providers
V.3.3	Stored data should be isolated from other systems or services, where possible.	Vendors, Service Providers, Integrators, Licensees
V.3.4	Device metadata should be trusted and verifiable.	Vendors
V.4	**Network security**	
Controls		Applies to
V.4.1	To build a secure environment the network should be segmented into logical groups and host-to-host communications paths should be restricted to those that are strictly necessary. This mitigates threats and failures spreading from compromised devices to other devices and networks.	Service Providers, Integrators, Licensees
V.4.2	As well as the protection of individual devices, measures should also be taken to protect high level systems. This includes determining at the design phase how to connect devices to the system and also employing services to protect each network, for example using firewalls and malware detection.	Service Providers, Integrators, Licensees
V.5	**Patch management**	
Controls		Applies to
V.5.1	Providers should consider that updates may fail and may cause devices to be in an inconsistent state. It is therefore desirable to be able to rollback devices to the last known working version remotely or, when this is not possible, using a local or manual rollback option with appropriate instructions for users to execute.	Vendors, Service Providers, Licensees

V.5.2	The ability to change any device's software should be restricted to authorized entities only, including the possibility to restore the device configuration, taking into account controls related to cryptography and system security.	Vendors
V.5.3	An inventory of devices may be necessary for the proper management of devices. For large quantities of devices, a proper segmentation by type of device or by geographical zone is advised. Note that this is dependent on the use of proper device identification and the ability to enable/disable updating using a secure and trusted channel, as given in further controls.	Vendors, Service Providers
V.5.4	V.5.4.1 - Updates and patches that are important for the security of IoT systems and services should be provided in a timely manner.	Vendors, Service Providers
	V.5.4.2 - Updates and patches should not modify user-configured preferences, security and or settings without user notification.	
	V.5.4.3 - Users should be informed about the changes that are to be applied in each update.	Vendors, Service Providers
	V.5.4.4 - Updates should be applied automatically by default, and users should not be allowed to disable an update when is related to device's or applications' security	Vendors, Service Providers
V.5.5	Users and providers should have clear visibility on a device’s patching and update status.	Vendors, Service Providers
V.5.6	The cybersecurity state of devices should be reported and a mechanism to recognize abnormal or degraded cybersecurity states should be employed.	Vendors, Service Providers
V.6	**Physical security**	
Controls		Applies to
V.6.1	Where possible, physical access to devices should be restricted. This includes external interfaces, service ports, wipe and reset buttons, removable memory cards and any removable part.	Vendors, Service Providers, Integrators, Licensees

V.7	**Policy / governance**	
Controls		Applies to
V.7.1	Users should be assisted in assuring that the data processing operations of their products are functioning as specified, including clear guidance on how to secure privacy settings without losing device functionality, for example via device manuals or websites. Users must be informed about what private data is required for the device to function properly.	Licensees
V.7.2	Consumers should be informed about the end-of-life policy of their products. This should include the minimum length of time in which a device will receive software updates and the consequences of not receiving updates. Also, users should be assisted in all stages of the cycle of life of the product, including installation, connection, operation and maintenance.	Integrators, Licensees
V.7.3	The functionality that the device offers and its intended use should be made clear to users, including any restrictions or limitations.	Vendors, Service Providers
V.8	**Privacy**	
Controls		Applies to
V.8.1	It should be clearly disclosed whether IoT device, product, or service ownership and the contained data may be transferred and how this may take place.	Vendors, Service Providers, Licensees
V.8.2	Ensure that personal identifiers are removed or anonymized, where necessary.	Vendors, Service Providers, Licensees
V.9	**Resilience**	
Controls		Applies to
V.9.1	Devices should be built in a resilient way such that they can be recovered in the case of outages of data networks or a loss of power. In these cases, the device should also remain operating and locally functional as far as reasonably possible.	Vendors, Service Providers

V.9.2	After an outage, devices should be able to return to a network in a sensible state and in an orderly fashion; mass scale reconnection should be avoided. IoT service providers should also update data when the network connection is restored.	Vendors, Service Providers
V.9.3	In the case of a failure of an individual device, other IoT devices must continue functioning as much as possible. The failed device should also disclose the reason for the failure.	Vendors
V.10	**Risk management**	
Controls		Applies to
V.10.1	Providers should specify original functions and information to be protected.	Vendors, Service Providers
V.10.2	V.11.2.1 - Risks in maintenance work and those resulting from the unauthorized use of maintenance tools should be assumed.	Vendors, Service Providers, Integrators, Licensees
	V.11.2.2 - When maintenance work is done by third parties, this should be supervised.	
V.11	**System monitoring**	
Controls		Applies to
V.11.1	In order to grant device management rights, each device should have a unique identifier that can be used to distinguish it from others. This logical identifier shall not be rewritable, spoofable or erasable in any way. A physical identifier may also represent the same value as the logical identifier.	Vendors
V.12	**System security**	
Controls		Applies to
V.12.1	Processes for updating and remote management should follow best security practice. For example; verifying that updates come from a trusted source using digital signatures, only applying signed updates and patches, and connecting to back-end applications only if they have been authenticated.	Vendors, Service Providers

V.12.2	Software should run with appropriate privileges, avoiding the use of a root or administrator account for non-privilege tasks. Advanced credentials should be only used only when necessary.	Vendors, Service Providers
V.12.3	Developers should mitigate the possibility for input data to break into the system. Any data from outside the system (from a user or other system) shall therefore be controlled to avoid exploits or arbitrary code injections. This may include control expected types (for example, executable code rather than a username) or ranges (for example, introducing more characters than expected), amongst others.	Vendors, Service Providers
V.12.4	Measures should be taken to protect user accounts against "brute force" and other abusive login attempts by delaying additional authentication attempts after too many failed attempts. It should be noted that the disabling of accounts after too many failed attempts can be used as a means for a DoS attack.	Vendors, Service Providers
V.12.5	Security should be part of the design of devices and applications. Devices should be built taking into account previously encountered attack vectors to prevent them from falling victim to common cyber-attacks such as DDoS or Trojans, and they should be secured in a way to prevent them becoming compromised to create botnets.	Vendors, Service Providers
V.12.6	The integrity of software on the device should be verified, for example via secure boot.	Vendors
V.12.7	Companies should have disaster recovery plans. These may include regular backups of data, including settings, and disaster recovery exercises, among other items.	Service Providers, Licensees
V.12.8	Functionality should be created to restrict access to the state indicator to authorized entities only and to make state information available to a service on another device such as an event/state log server.	Vendors, Service Providers
V.12.9	Where applicable, the implicated risks of the improper use of devices should be reported to users along with important security points to reduce such risk.	Vendors, Service Providers, Licensees
V.12.10	Installation and maintenance of IoT devices should cover the minimal security steps and must follow security best practice on usability.	Vendors

V.12.11	Provide users with notification of password resets or changes that require secure authentication.	Vendors, Service Providers
V.12.12	IoT devices should provide notice and/or request user-confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services.	Vendors, Service Providers
V.13	**Vulnerability management**	
Controls		Applies to
V.13.1	A breach, cyber response and consumer notification plan should be enacted. Such a plan should be revaluated, tested and updated annually and also after any significant internal system changes.	Vendors, Service Providers
V.13.2	Regular penetration testing, threat modelling and monitoring should be performed to maintain awareness of vulnerabilities and maintain continuous improvement.	Vendors
V.13.3	Compromised or malfunctioning devices should be identified and revoked.	Vendors
V.13.4	Bug bounty programs should encourage the cyber security community to identify and report vulnerabilities. It is advised that a well-recognized bug bounty platform is used for this to make it easier.	Vendors, Service Providers

Terms and Definitions

Term	Definition
Access Management	Framework of policies, processes, and relevant technologies that give the right users the appropriate access permissions in order to avoid misuse of access privileges.
Authentication	The process of verification required for the identity of users, processes, or devices which request access to a particular technology resource.
Backup	Copies of data and devices stored elsewhere which can be retrieved to restore the original versions in the event of failure or deletion.

Botnet	Internet-connected computers infected by malware that are controlled as a group by malicious actors outside the knowledge of owners of infected computers.
Configuration management	A system management process which establishes and maintains consistency of a system or software through automated methods and procedures.
Cryptography	Rules and methods used to encrypt information that can be decrypted only by intended user/device to prevent unauthorized use as well as loss of its confidentiality and integrity during transit and storage.
Data storage / protection	Means of relocating inactive data to a dedicated archive in the form of a device which retains such data for a prolonged period of time.
Event	Any occurrence that has significance for the functioning of a system’s hardware or software.
Firewall	A network security system which can monitor, filter, and control inbound and outbound traffic based on a predetermined set of rules.
Identification	The means of verifying the identity of users, processes, or devices which request access to a particular technology resource.
Integrator	Companies that act ask the middleman between IoT services and devices by integrating such components to client networks / systems.
Integrity	Defines the state of information being authentic and not modified to lose its authenticity partially or fully.
IoT Service Provider	Specialized companies that develop and offer only IoT services.
Licensee	Any telecommunication service provider in Oman holding a Class 1, 2, or 3 license from TRA.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or of otherwise annoying or disrupting the victim.

Multi-factor authentication	A multi-factor electronic authentication mechanism requiring more than one authentication factor which is used to verify the identity of a user and grant access to the requested device or process.
Network security	The practice of safeguarding networks, including the IT infrastructure and resources that are accessed by the network.
Patch management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.
Physical security	The measures developed to secure the physical assets of an organization or entity. Physical security measures include prevention of unauthorized access to organization’s premises, equipment and resources, as well as protection of such assets from harm or damage.
Policy / governance	A Policy is a formal document outlining the commitment of an organization to a defined objective or direction. In the context of cybersecurity, a cybersecurity policy and governance document express such a commitment to enhance the cybersecurity level of the organization by setting clear objectives and requirements.
Privacy	Lack of unauthorized disclosure or alteration of personal information of individuals.
Recovery	The process of restoring something to its original state after it has been damaged, stolen, lost, or suspended.
Resilience	In the context of cybersecurity, resilience refers to the ability to resist cyber-attacks from causing damage or harm, and to recover from their effects easily in due time.
Risk management	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: 1) the conduct of a risk assessment, 2) the implementation of a risk mitigation strategy; and 3) employment of techniques and procedures for the continuous monitoring of the security state of the information system

System monitoring	Tracking of system resources and analysis of existing and potential extraordinary traffic activity which might point to cyber threats for the organization.
System security	The process of protection of system resources from unauthorized access, disclosure, modification, and destruction of information.
Threat	An event which may have a negative impact on an organization’s operations, assets, and other resources (including individuals) by various means. In the context of cybersecurity, threats may stem from unauthorized access to an information system and the loss of confidentiality, integrity, or availability of information.
Vendor	Providers of IoT-related hardware and software both for the back end and user side.
Vulnerability management	A weakness in a system, application, or network that is subject to exploitation or misuse.

List of abbreviations

Abbreviation	Full term
CCTV	Closed Circuit Television
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
FIPS	Federal Information Processing Standards
ICT	Information and Communication Technology
IoT	Internet of Things
OWASP	Open Web Application Security Project
TRA	Telecommunications Regulatory Authority

Consultation Questions

1. **Do you agree with TRA on the compliance requirement (mandatory / voluntary) of each IoT security control and sub-control outlined in the Standard? If not, please provide your justified view on the matter.**

2. **From the point of view of a vendor, do you agree that the mandatory and voluntary controls applicable to vendors are appropriate? If not, please provide the changes you think are needed and their justification.**

3. **From the point of view of an IoT service provider, do you agree that the mandatory and voluntary controls applicable to IoT service providers are appropriate? If not, please provide the changes you think are needed and their justification.**

4. **From the point of view of an integrator, do you agree that the mandatory and voluntary controls applicable to integrators are appropriate? If not, please provide the changes you think are needed and their justification.**

5. **From the point of view of a licensee, do you agree that the mandatory and voluntary controls applicable to licensees are appropriate? If not, please provide the changes you think are needed and their justification.**

6. **Do you see any ambiguity in the applicability of certain controls to your entity, or do you feel that responsibility for any such controls should be borne by other stakeholders instead?**

7. **Are there any other IoT security domains or controls you think should be included in this Standard? If yes, please provide the relevant domains or controls and your justified view for each.**

8. **Do you think any of the IoT security domains or controls should be removed from this Standard? If yes, please provide the relevant domains or controls and your justified view for each.**

9. **How much time do you think is required for your organization to fully implement the applicable mandatory controls?**

10. **Do you anticipate requiring support for the implementation of the mandatory controls to your organization?**