Security Requirement		☆1 Security Requirement	☆1 Conformance	☆1 Conformance Criteria	Conditions for N/A (Non-applicable), Supplementary Explanation	☆1 Evaluation Method	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement							
1. No universal default passwords	1-1. Where passwords are used and in any state other than the factory default, all passwords shall be unique per device or defined by the user.	✓	–	*Integrated into the conformance criteria for conformance item #2.*	–	–	[ETSI EN 303 645]5.1-1 M C (1) [UK: PSTI Act]SCHEDULE 1: 1-(2) [US: NISTIR 8425]Interface Access Control 1-b [Singapore: CLS][*]5.1-1 [IEC 62443-4-2]CR1.5, CR1.7	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (2) [CCDS Certification]1-1 Access Control and Authentication [Mandatory] 2), 1-1-2 Change of credentials [Mandatory] 2) [BMSec]IA-2 b)-2), e)-2) 2.2) [JISEC-C0755]FMT_IPWD_EXT
1. No universal default passwords	1-2. Where pre-installed unique passwords are used, these shall be sufficiently randomized against automated attacks.	✓	2	For products that use passwords or passcodes in the user authentication mechanism via a network against the device or in the client authentication mechanism at initial setup of the device, either of the following criteria (1) or (2) shall be met when default passwords are used at the time of product installation: (1) The default password shall be unique per device and shall be at least 6 characters long and not easily guessable. (2) The default password shall implement a function that requires the user to change the password when the product is first started up, and shall force the user to set a password of 8 or more characters as a password that can be set in such function.	Conditions for N/A: No mechanism for user authentication via a network (Provide rationale as to why user authentication is not necessary to counter threats in "Reasons for N/A")	Document: (1) (2) Device check: None	[ETSI EN 303 645]5.1-2 M C (2) [UK: PSTI Act]SCHEDULE 1: 1-(3) [Singapore: CLS][＊]5.1-2 [IEC 62443-4-2]CR1.7	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (2) [CCDS Certification]1-1 Access Control and Authentication [Mandatory] 2) [JISEC-C0755]FMT_IPWD_EXT
1. No universal default passwords	1-3. Authentication mechanisms used to authenticate users against the product shall use technologies that reduce the assumed risks appropriate to the properties of the product usage etc.	✓	1	Access to information assets to be protected by users or other devices via TCP/UDP communications shall be made by access control based on appropriate authentication mechanisms. ** **Products that have received certification for conformity to the technical regulations specified in the Telecommunications Business Act including the Technical Standards for Terminal Equipment Security (products to which the Technical Standards Conformity T Mark or A Mark is affixed) shall be deemed to conform to this criteria. (In this case, enter the Technical Standards Conformity Approval number etc. based on the Telecommunications Business Law in the "Basic Information" sheet (the Design Certification number for the Technical Standards Conformity T Mark or the Technical Standards Conformity Approval number for the [A] Mark)".)	Conditions for N/A: No mechanism for authentication and access via TCP/UDP communications for access to information assets to be protected (Provide rationale as to why authentication and access are not necessary to counter unauthorized external access in "Reasons for N/A") Definition of term: "information assets to be protected" include all of the following information ・Configuration information related to communication functions ・Configuration information related to security functions ・Information that is generally sensitive, such as personal information, that is collected, stored, or communicated by the device in the intended use of the device.	Document : Yes Device check: None	[ETSI EN 303 645]5.1-3 M [UK: PSTI Act]SCHEDULE 1: 1-(3) [US: NISTIR 8425]Interface Access Control2-b [EU: CRA]ANNEX I 1.(3)(b) [Singapore: CLS][＊]5.1-3 [IEC 62443-4-2]CR1.5	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (1) [CCDS Certification]1-1 Access Control and Authentication [Mandatory] 4), 1-2 Data Protection[Mandatory] 3) [RBSS]Certification Standard for Security Camera 5.2.12 (2), Certification Standard for Digital Recorder（Security Uses） 5.2.12 (2) [JISEC-C0755]FIA_UAU, FMT_SMR

Security Requirement		☆1 Security Requirement	☆1 Conformance	☆1 Conformance Criteria	Conditions for N/A (Non-applicable), Supplementary Explanation	☆1 Evaluation Method	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement							
1. No universal default passwords	1-4. For user authentication against the product, the products shall provide to the user or an administrator a simple mechanism to change the authentication value used.	✓	3	Enables changing the authentication value for user authentication via a network against the device, regardless of authentication type (password, token, fingerprint, etc.).	Conditions for N/A: No mechanism for user authentication via a network (Provide rationale as to why user authentication is not necessary to counter unauthorized external access in "Reasons for N/A") Definition of term: "authentication value" The individual value of an attribute used by the authentication mechanism to the product. (e.g., for a password-based authentication mechanism, the authentication value is a string of characters. In the case of biometric fingerprint authentication, the authentication value is, for example, the fingerprint data of the index finger of the left hand).	Document: Yes Device check: None	[ETSI EN 303 645]5.1-4 M C (8) [Singapore: CLS][＊]5.1-4 [IEC 62443-4-2]CR1.5	[CCDS Certification]1-1-2 Change of credentials [Mandatory] 1) [BMSec]IA-2 [RBSS]Certification Standard for Digital Recorder（Security Uses） 5.2.12 (2) [JISEC-C0755]FMT_IPWD_EXT
1. No universal default passwords	1-5. When the device is not a constrained device, it shall have a mechanism available which makes brute-force attacks on authentication mechanisms via a network impracticable.	✓	4	When the device is not a constrained device, the user authentication mechanism via a network against the device shall be a mechanism which makes brute-force attacks difficult.	Conditions for N/A: One of the following conditions applies. (OR Condition) ・There is no mechanism for user access to the equipment via a network (Provide a rationale as to why user access is not necessary to counter unauthorized external access in "Reasons for N/A") ・The device falls under the category of "restricted equipment" (Provide evidence that the device falls under the category of "restricted equipment" in "Reasons for N/A") Definition of term: "constrained device" A device which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use.	Document: None Device check: Yes	[ETSI EN 303 645]5.1-5 M C (5) [EU: CRA]ANNEX I 1.(3)(b) [Singapore: CLS][＊]5.1-5 [IEC 62443-4-2]CR1.11	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (1) [CCDS Certification]1-1 Access Control and Authentication [Mandatory] 3) [BMSec]IA-3 [JISEC-C0755]FIA_AFL
2. Managing vulnerability reports	2-1. The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum: • contact information for the reporting of issues; and • information on timelines for: 1) initial acknowledgement of receipt; and 2) status updates until the resolution of the reported issues.	✓	5	The manufacturer shall make a vulnerability disclosure policy publicly available (e.g. post on the manufacturer's website) that includes all of the following information (1) through (3). (1) Contact information for the reporting of product security issues to the manufacturer (e.g. manufacturer's website URL, phone number, email address) (2) Procedures to be followed by the manufacturer after receipt of a report on the security of the product and an outline of such procedures. (3) Any procedures regarding product and vulnerability status updates until the vulnerability is resolved, and an outline of such procedures.	–	Document: (1) (2) (3) Device check: None	[ETSI EN 303 645]5.2-1 M [UK: PSTI Act]SCHEDULE 1: 2-(2), 2-(3) [US: NISTIR 8425]Information & Query Reception1, 1-a, 1-b, Product Education & Awareness [EU: CRA]ANNEX I 2.(5), ANNEX I 2.(6), ANNEX II 1, ANNEX II 2 [Singapore: CLS][＊]5.2-1 [IEC 62443-4-1]DM-1	[CCDS Certification]2-1 Contact point and security support system [Mandatory] 1) [BMSec] FR-1

Security Requirement		☆1 Security Requirement	☆1 Conformance	☆1 Conformance Criteria	Conditions for N/A (Non-applicable), Supplementary Explanation	☆1 Evaluation Method	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement							
3. Keep software updated	3-1. Particular software components included in products shall be updateable.	✓	6	All of the following criteria (1) through (3) shall be met for the update function of the software components included in the product. ** (1) The firmware (software) package of the product shall be updateable. (2) The firmware (software) package shall have a means to confirm that the latest firmware (software) is installed, such as being able to check the version of the firmware (software) package. (3) The version of the firmware (software) package that has been updated shall be kept up-to-date even after power-off. **Products that have received certification for conformity to the technical regulations specified in the Telecommunications Business Act including the Technical Standards for Terminal Equipment Security (products to which the Technical Standards Conformity T Mark or A Mark is affixed) shall be deemed to conform to this criteria. (In this case, enter the Technical Standards Conformity Approval number etc. based on the Telecommunications Business Law in the "Basic Information" sheet (the Design Certification number for the Technical Standards Conformity T Mark or the Technical Standards Conformity Approval number for	–	Document: None Device check: (1) (2) (3)	[ETSI EN 303 645]5.3-1 R [US: NISTIR 8425]Software Update 1 [EU: CRA]ANNEX I 2.(8) [Singapore: CLS][＊＊＊]CK-LP-03 [IEC 62443-4-1]SM-6, SUM-1 [IEC 62443-4-2]CR4.3, CR3.10 EDR3.10, HDR3.10 NDR 3.10	[CCDS Certification]1-3 Software Update [Mandatory] 1) [Recommended] 1) [BMSec]PT-1 [JISEC-C0755]FMT_SMF
3. Keep software updated	3-2. When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.	✓	–	*Integrated into the conformance criteria for conformance items #6 and #8.*	–	–	[ETSI EN 303 645]5.3-2 M C (5) [US: NISTIR 8425]Software Update 1 [Singapore: CLS][＊]5.3-2	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (3) [CCDS Certification]1-3 Software Update [Mandatory] 1) [Recommended] 1) [BMSec]PT-1 b)-3) [JISEC-C0755]FMT_SMF
3. Keep software updated	3-3. When the product implements an update mechanism, the update shall be simple for the user to apply.	✓	7	The product enables users to perform software updates in a simple and understandable procedure when applying updates.	–	Document: Yes Device check: None	[ETSI EN 303 645]5.3-3 M C (12) [EU: CRA]ANNEX I 2.(8) [Singapore: CLS][＊]5.3-3 [IEC 62443-4-1]SUM-4	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (3) [BMSec]PT-1 b)-4), e)-1) [JISEC-C0755]FMT_SMF
3. Keep software updated	3-7. When the product implements an update mechanism, the product shall use best practice cryptography to facilitate secure update mechanisms.	✓	8	When updating software via a network, there shall be a mechanism to verify the software integrity prior to updating.	Conditions for N/A: No mechanism for updating software via a network (Describe the expected update mechanism in "Reasons for N/A")	Document: Yes Device check: None	[ETSI EN 303 645]5.3-7 M C (12) [US: NISTIR 8425]Software Update 1 [Singapore: CLS][＊]5.3-7 [IEC 62443-4-2]CR4.3	[CCDS Certification]1-3 Software Update [Recommended] 2) [JISEC-C0755]FMT_SMF
3. Keep software updated	3-8. When the product implements an update mechanism, security updates shall be timely.	✓	9	The manufacturer shall document policies and guidelines for prioritizing security updates to achieve rapid updates to security issues.	–	Document: Yes Device check: None	[ETSI EN 303 645]5.3-8 M C (12) [EU: CRA]ANNEX I 2.(2), ANNEX I 2.(7), ANNEX I 2.(8) [Singapore: CLS][＊]5.3-8 [IEC 62443-4-1]SUM-5	[CCDS Certification]2-1 Contact point and security support system [Mandatory] 2) [BMSec]PT-1 b)-4), e)-1) [JISEC-C0755]FMT_SMF
3. Keep software updated	3-10. Where updates are delivered over a network interface, the product shall verify the authenticity and integrity of each update via a trust relationship.	✓	–	*Integrated into the conformance criteria for conformance item #8.*	–	–	[ETSI EN 303 645]5.3-10 M (11,12) [EU: CRA]ANNEX I 1.(3)(e) [Singapore: CLS][＊]5.3-10 [IEC 62443-4-1]SM-6 [IEC 62443-4-2]CR3.1, CR3.2 SAR3.2, EDR3.2 HDR3.2, NDR3.2	[CCDS Certification]1-3 Software Update [Recommended] 1) [JISEC-C0755]FMT_SMF

Security Requirement		☆1 Security Requirement	☆1 Conformance	☆1 Conformance Criteria	Conditions for N/A (Non-applicable), Supplementary Explanation	☆1 Evaluation Method	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement							
3. Keep software updated	3-14. The model designation of the products shall be clearly recognizable, either by labelling on the product or via a physical interface.	✓	10	The model number of the product shall be provided to the users in any of the following ways. (1) The model number of the product shall be written directly on the product itself. (2) Users shall be able to recognize the model number from the GUI, web UI, etc. of the product, or from the GUI, web UI, etc. of software or applications (e.g., smartphone applications) attached to the product.	–	Document: None Device check: (1) or (2)	[ETSI EN 303 645]5.3-16 M [US: NISTIR 8425]Information Dissemination 2 [EU: CRA]ANNEX II 3 [Singapore: CLS][＊]5.3-16	
4. Securely store sensitive parameters	4-1. Sensitive security parameters in the product's storage shall be stored securely by the product.	✓	11	Information assets to be protected that are stored in product storage (including information assets to be protected that are stored in storage media such as SD cards, etc.) shall be securely stored against unauthorized access via a network.	Definition of term: "information assets to be protected" include all of the following information ・Configuration information related to communication functions ・Configuration information related to security functions ・Information that is generally sensitive, such as personal information, that is collected, stored, or communicated by the device in the intended use of the device.	Document: Yes Device check: None	[ETSI EN 303 645]5.4-1 M [US: NISTIR 8425]Data Protection 1, Interface Access Control 2-a [Singapore: CLS][＊＊]5.4-1 [IEC 62443-4-2]CR1.5, CR1.9, CR1.14, CR3.8, CR4.1, CR3.12 EDR3.12 HDR3.12 NDR3.12, CR3.13 EDR3.13 HDR3.13 NDR3.13	[CCDS Certification]1-2 Data Protection[Mandatory] 1) 3) [JISEC-C0755]FMT_MTD
5. Communicate securely	5-1. The product shall use best practice cryptography to communicate securely.	✓	12	For information assets to be protected that are transmitted via a network, one of the following protection measures against information eavesdropping shall be implemented. (1) For information assets to be protected that are transmitted via a network to other IoT devices or servers (including servers in the cloud), the device themselves shall take protective measures against information eavesdropping. (2) For information assets to be protected that are transmitted via a network to other IoT devices or servers (including servers in the cloud), the information assets shall be transmitted only in a protected communication environment (VPN environment or connection environment via leased line).	Conditions for N/A: No information assets to be protected are transmitted via a network. (Provide evidence that there are no information assets to be protected transmitted via a network in "Reasons for N/A") Definition of term: "information assets to be protected" include all of the following information ・Configuration information related to communication functions ・Configuration information related to security functions ・Information that is generally sensitive, such as personal information, that is collected, stored, or communicated by the device in the intended use of the device.	Document: (1) or (2) Device check: None	[ETSI EN 303 645]5.5-1 M [US: NISTIR 8425]Data Protection 3 [EU: CRA]ANNEX I 1.(3)(c) [Singapore: CLS][＊＊]5.5-1 [IEC 62443-4-2]CR3.1, CR4.3	[CCDS Certification]1-2 Data Protection[Mandatory] 2), 1-4-1 Wi-Fi authentication method [Mandatory] 1), 1-4-2 Bluetooth vulnerability countermeasures [Mandatory] 1) [BMSec]TP-1
5. Communicate securely	5-5. Product functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the product and where the manufacturer cannot guarantee what configuration will be required for the product to operate.	✓	–	*Integrated into the conformance criteria for conformance item #1.*	–	–	[ETSI EN 303 645]5.5-5 M [EU: CRA]ANNEX I 1.(3)(b) [Singapore: CLS][＊＊]5.5-5 [IEC 62443-4-2]CR1.6 NDR1.6, CR2.12, CR6.1	[CCDS Certification]1-1 Access Control and Authentication [Mandatory] 4), 1-1-1 Disabling of TCP/UDP ports [Recommended] 2), 1-3 Software Update [Recommended] 3) [BMSec]IA-1, MT-1 [RBSS]Certification Standard for Security Camera 5.2.12 (2)-4, Certification Standard for Digital Recorder (Security Uses) 5.2.12 (2)-4 [JISEC-C0755]FAU_UID

Security Requirement		☆1 Security Requirement	☆1 Conformance	☆1 Conformance Criteria	Conditions for N/A (Non-applicable), Supplementary Explanation	☆1 Evaluation Method	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement							
5. Communicate securely	5-7. The product shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.	✓	–	*Integrated into the conformance criteria for conformance item #12.*	–	–	[ETSI EN 303 645]5.5-7 M [EU: CRA]ANNEX I 1.(3)(c) [Singapore: CLS][＊＊]5.5-7 [IEC 62443-4-2]CR3.1, CR4.3	[CCDS Certification]1-2 Data Protection[Mandatory] 2), 1-4-1 Wi-Fi authentication method [Mandatory]
6. Minimize exposed attack surfaces	6-1. All unused network physical interfaces and logical interfaces shall be disabled.	✓	13	In order to reduce the risk of external cyberattacks, physical interfaces and logical interfaces that are unnecessary for the use of the product and are at risk of being attacked shall be disabled, and vulnerability assessments shall be performed on the product. Specifically, all of the following criteria (1) and (2) shall be met. (1) For the following interfaces that are used frequently in the product and are assumed to be at risk such as via a vulnerability, the interfaces that are unnecessary for the use of the product and are at risk of being attacked shall be disabled. A) TCP/UDP port B) Bluetooth C) USB (2) The product shall be inspected for known vulnerabilities by vulnerability scanning tools and vulnerabilities that could be exploited shall not be detected.	–	Document: (1) Device check: (1) (2) **(1) requires both document and device check	[ETSI EN 303 645]5.6-1 M [US: NISTIR 8425]Interface Access Control 1-a [EU: CRA]ANNEX I 1.(3)(h) [Singapore: CLS][＊＊]5.6-1 [IEC 62443-4-2]CR7.7	[CCDS Certification]1-1-1 Disabling of TCP/UDP ports [Mandatory] 1) [BMSec]NI-1, VA-1, VA-2, VA-3
9. Resilience to outages	9-1. Resilience shall be built into the products and services, taking into account the possibility of outages of data networks and power.	✓	14	When the power supply and network functions are restored after the device is turned off due to a power or network outage, the settings of authentication values (passwords, secret keys, etc.) used for access control and the software that has been updated shall maintain the state immediately before the power-off, without returning to the factory default state. **Products that have received certification for conformity to the technical regulations specified in the Telecommunications Business Act including the Technical Standards for Terminal Equipment Security (products to which the Technical Standards Conformity T Mark or A Mark is affixed) shall be deemed to conform to this criteria. (In this case, enter the Technical Standards Conformity Approval number etc. based on the Telecommunications Business Law in the "Basic Information" sheet (the Design Certification number for the Technical Standards Conformity T Mark or the Technical Standards Conformity Approval number for the [A] Mark)".)	–	Document: None Device check: Yes	[ETSI EN 303 645]5.9-1 R [EU: CRA]ANNEX I 1.(3)(f) [IEC 62443-4-2]CR7.1, CR7.3	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (4) [CCDS Certification]1-1 Access Control and Authentication [Mandatory]⑤

Security Requirement		☆1 Security Requirement	☆1 Conformance	☆1 Conformance Criteria	Conditions for N/A (Non-applicable), Supplementary Explanation	☆1 Evaluation Method	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement							
11. Delete user data	11-1. The user shall be provided with functionality such that user data can be erased from the product in a simple manner.	✓	15	All of the following criteria (1) and (2) shall be met for the delete function of data stored in product storage during the use of the product. (1) The user can delete at least the following data related to the user via the device itself or associated services (such as a mobile application) A) information assets (including personal information) obtained during the use of the product B) user configuration values C) authentication values set by user, cryptographic keys and digital signatures obtained during use of the product (2) The updated version of firmware (software) package related to security features shall be maintained after data deletion	–	Document: (1) Device check: (1) (2) **(1) requires both document and device check	[ETSI EN 303 645]5.11-1 M [US: NISTIR 8425]Data Protection 2 [Singapore: CLS][＊＊]5.11-1 [IEC 62443-4-2]CR4.2	[CCDS Certification]1-2-1 Data erasure function [Mandatory] 1) [BMSec]MT-2 [JISEC-C0755]FMT_MTD
17. Provide information on products	17-2. The manufacturer shall provide users with guidance on how to securely set up, use and dispose of their products.	✓	16	The manufacturers shall meet all of the following criteria (1) through (5) to provide information regarding the cybersecurity of products. (1) The procedures for safe use of the product, such as initial setup procedures, and other settings and usage procedures that may affect cybersecurity in the use of the product, shall be made known to the public. (2) The content and necessity of product security updates and the consequences of not updating the product shall be made known to the public. (3) They shall make disclaimers known of accidents or failures that can be expected if updates are not made, and of accidents or failures that can generally be expected. (4) They shall make known the policy when the support for the target product or service expires or is terminated. (5) They shall make known the assumed risk associated with disposal or resale of the product with residual information assets to be protected, and how to safely terminate use of the product, including data removal.	Definition of term: "information assets to be protected" include all of the following information ・Configuration information related to communication functions ・Configuration information related to security functions ・Information that is generally sensitive, such as personal information, that is collected, stored, or communicated by the device in the intended use of the device.	Document: (1) (2) (3) (4) (5) Device check: None	[ETSI EN 303 645]5.12-2 R [US: NISTIR 8425]Documentation 1-a, 1-d, Product Education & Awareness 1-a, Information Dissemination 2 [EU: CRA]ANNEX II 4, ANNEX II 9 [IEC 62443-4-1]SUM-2	[CCDS Certification]2-3 Provision of information to users [Mandatory] 1) [BMSec]PT-1, TP-1
17. Provide information on products	17-3. The manufacturer shall inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update.	✓	–	*Integrated into the conformance criteria for conformance item #16.*	–	–	[ETSI EN 303 645]5.3-11 R C (12) [US: NISTIR 8425]Information Dissemination 1c 1d 1e [EU: CRA]ANNEX I 2.(4), ANNEX I 2.(8) [IEC 62443-4-1]SUM-2	[CCDS Certification]2-3 Provision of information to users [Mandatory] 2) [BMSec]FR-2
17. Provide information on products	17-5. The manufacturer shall provide the user with a specified procedure for disposing of the product.	✓	–	*Integrated into the conformance criteria for conformance item #16.*	–	–	[US: NISTIR 8425]Product Education & Awareness 1-c [IEC 62443-4-1]SG-4	[CCDS Certification]2-3 Provision of information to users [Mandatory]⑤ [BMSec]DP-1

Security Requirement		☆1 Security Requirement	☆1 Conformance	☆1 Conformance Criteria	Conditions for N/A (Non-applicable), Supplementary Explanation	☆1 Evaluation Method	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement							
17. Provide information on products	17-8. The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.	✓	–	*Integrated into the conformance criteria for conformance item #16.*	–	–	[ETSI EN 303 645]5.3-13 M [UK: PSTI Act]SCHEDULE 1: 3-(2), 3-(3), 3-(4) [US: NISTIR 8425]Product Education & Awareness 1-d, 1-e, Information Dissemination 1b [EU: CRA]ANNEX II 6, ANNEX II 7, ANNEX II 8 [Singapore: CLS][＊]5.3-13 [IEC 62443-4-1]SG-3	[CCDS Certification]2-3 Provision of information to users [Mandatory] 4) [JISEC-C0755]FPT_SMT
17. Provide information on products	17-10. The manufacturer shall provide the user with information in a specified manner regarding product usage that may pose a security risk.	✓	–	*Integrated into the conformance criteria for conformance item #16.*	–	–	[US: NISTIR 8425]Documentation 1-d [EU: CRA]ANNEX II 5 [IEC 62443-4-1]SG-3, SR-1	[CCDS Certification]2-3 Provision of information to users [Mandatory] 1) 3) [BMSec]PR-1