IoT Devices Security Requirements Guidelines 2023: CCDS-GR01-2023 Ver. 1.0

General Incorporated Association
Connected Consumer Device Security Council

December 28, 2022

Update History

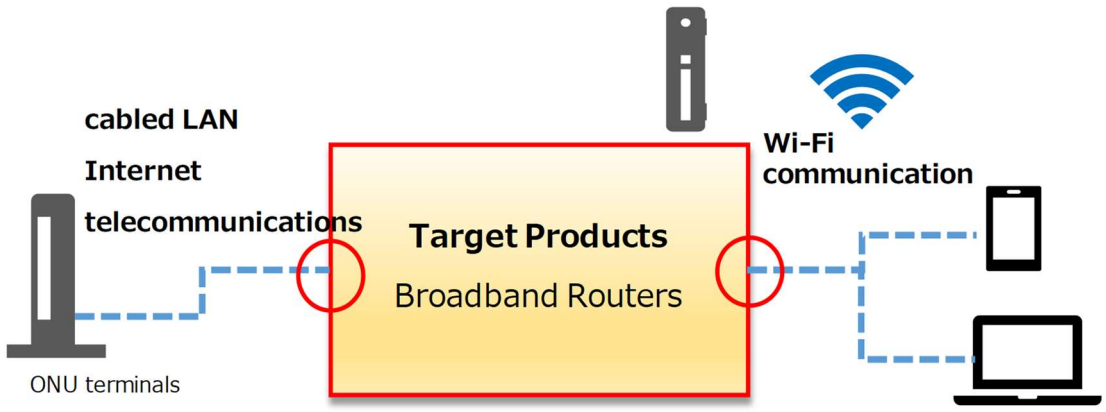
Revision	Date of Update	Description of Update	Formulated by
Rev. 1.0	Dec. 28, 2022	Ver. 1.0 release	CCDS

1. Purpose of This Document

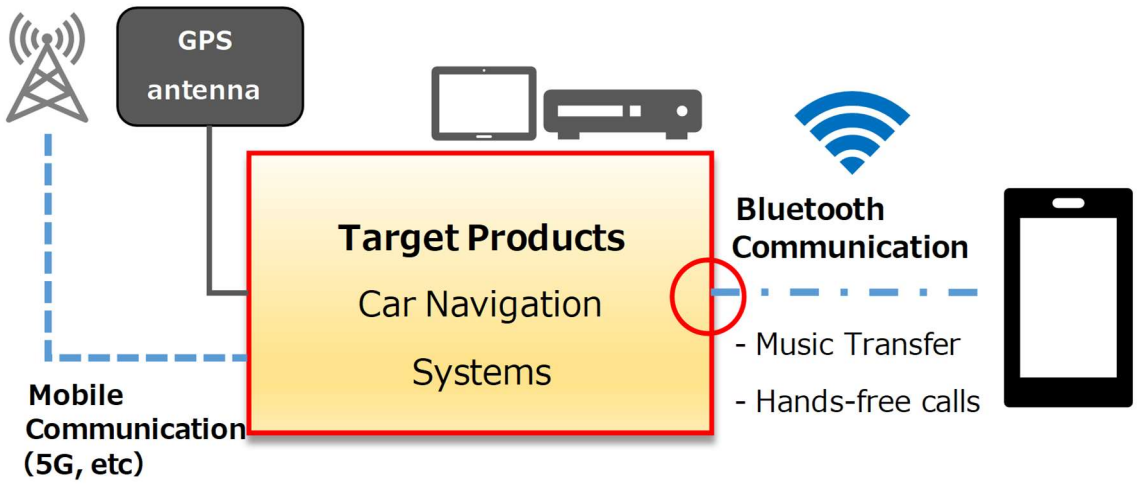
This Guidelines defines a minimum set of requirements (action level: ★) to be satisfied by connected devices. These minimum requirements are to apply to IoT device and system implementations of connected devices.

2. Scope of Granting of the CCDS Certification Mark

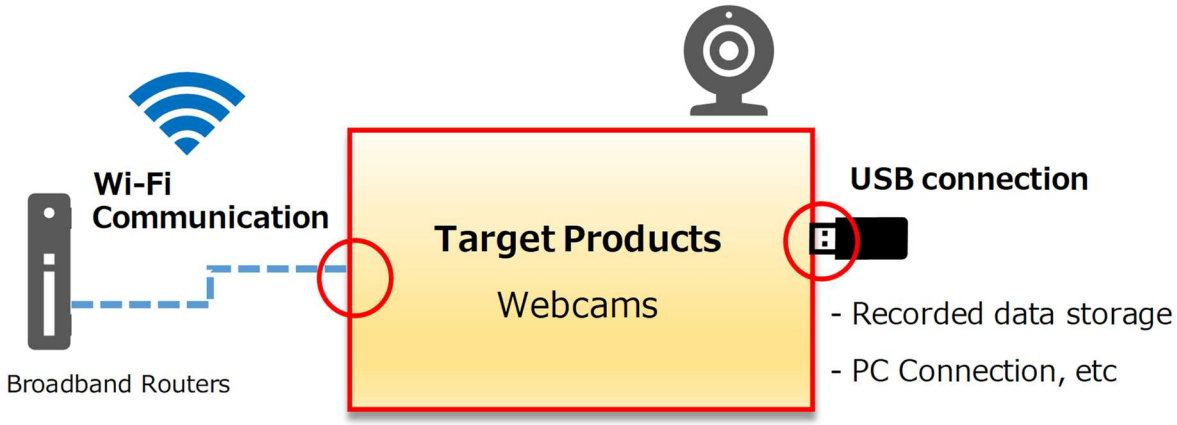
The scope of granting of the CCDS Certification Mark encompasses those devices and systems with Internet Protocol-ready hardware and software interfaces. It also covers devices and systems with Wi-Fi, Bluetooth, and/or USB interfaces (see Figures 1 to 3 below), because relatively more vulnerabilities and attacks related to these interfaces are observed among IoT devices.



[Figure 1] Example 1 of certification-eligible products that implement a subject interface: Broadband Routers



[Figure 2] Example 2 of certification-eligible products that implement a subject interface: Car Navigation Systems



[Figure 3] Example 3 of certification-eligible products that implement a subject interface: Webcams

3. IoT Device Security Requirements

The requirements of the IoT Device Security Requirements_2023 Edition (CCDS-GR01-2023) are summarized in Table 1. Details on each IoT device security requirement is provided in Table 2.

[Table 1] CCDS IoT Device Security Requirements_2023 Edition (CCDS-GR01-2023) List

Classification	ID	Security Requirements (subset ID, security requirements)		Objectives and purpose
1. Functional requirements for IoT devices	1-1	Access Control and Authentication		Identification, access control, configuration change, privilege management, authentication
		1-1-1	Disabling of TCP/UDP ports	
		1-1-2	Change of credentials	
	1-2	Data Protection		Data protection, protection of credentials and key information
		1-2-1	Data erasure function	
	1-3	Software Update		Operational incident response
	1-4	Requirements with a particularly large number of incidents and high impact		
		1-4-1	Wi-Fi authentication method	
		1-4-2	Bluetooth vulnerability countermeasures	
		1-4-3	USB access control	
		1-4-4	Injection countermeasures	
2. Requirements for the operation of IoT devices	2-1	Contact point and security support system		Operational incident response
	2-2	Product document management		Documentation of security activities
	2-3	Provision of information to users		Operational support
3. Requirements for auditing IoT devices	3-1	Audit log recording		Operational incident response
		3-1-1	Time management function	

[Table 2] Details of individual IoT device security requirements

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
1. Functional requirements for IoT devices						
1-1		change	Access Control and Authentication	**Mandatory requirements** 1) Have an ID that allows users (general users and privileged users) and other IoT devices to uniquely identify the target device. 2) Enforce appropriate authentication or access control for access from users and other IoT devices for TCP/UDP communication that is necessary for system operation. For authentication, the default password shall be unique to each device. 3) Take countermeasures against consecutive login attempts in user authentication, e.g., sending alert notifications to privileged users, equipment operators or maintenance personnel when login attempts exceed a certain number	CWE-287: Improper Authentication CWE-264: Permissions, Privileges, and Access Controls	**[Threat background]** Appropriate authentication or communication access control in TCP/UDP sessions is not performed for the open ports required for system operation. Various problems such as information leakage of device data and privilege escalation (management functionality under control) could occur. **[Example]** - Wi-Fi wireless router, IP camera, etc. **[Reference]** **Technical standards conformity approval (Telecommunications Business Act)** **Related requirements** - Article 34 (10-1) Access control function - Article 34 (10-4) Access control function during power outage, software maintenance function **NIST IR8425 Related requirements**

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
				of times, or disabling the target account for a certain period of time. 4) Identify and authenticate users for functions that enable to change significant configurations, including device security-related functions to restrict anyone other than privileged users, device operators or maintenance personnel from executing the functions. 5) After network communication is broken, re-establish the connection with other devices in a secure state through the access control and/or authentication processes. **Recommended requirements** None		#1 Asset Identification #2 Product Configuration #4 Interface Access Control **ETSI EN 303 645 Related requirements** 5.1 No universal default passwords 5.4 Securely store sensitive security parameters 5.5 Communicate securely 5.9 Make systems resilient to outages
1-1	1-1-1	Change	Disabling of TCP/UDP ports	**Mandatory requirements** 1) Close TCP/UDP ports not used for system operation. 2) Regarding ports that need to be	CWE-671: Lack of Administrator Control over	**[Threat background]** By leaving unnecessary TCP/UDP ports open, communication that might possibly be exploited for cyberattacks could be

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
				opened for system operation, demonstrate that they meet the specified conformity criteria through vulnerability inspection. **Recommended requirements** 1) Implement a function that can identify open TCP/UDP ports and change open/close. 2) Restrict anyone other than privileged users, equipment operators or maintenance personnel from executing functions that open/close TCP/UDP ports.	Security	enabled. **[Example]** - Wi-Fi wireless router, IP camera, etc. **[Reference]** **NIST IR8425 Related requirements** *No relevant requirements specified **ETSI EN 303 645 Related requirements** 5.6 Minimize exposed attack surfaces
1-1	1-1-2	Change	Change of credentials	**Mandatory requirements** 1) Implement a function to change credentials such as user IDs and passwords, and ensure that the credentials are not hard-coded. 2) Implement a function that requires the user to change the password when the target of verification starts for the first time if the	CWE-259: Use of Hard-coded Password CWE-255: Credentials Management Errors	**[Threat background]** If credentials such as IDs and passwords required in accessing the device and/or its applications are hard-coded or cannot be changed through the configuration anyway, it is not possible to address the case where the credentials are compromised, which would lead to vulnerability.

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
				default password is not unique to each target of verification. 3) Restrict those other than privileged users, equipment operators or maintenance personnel from changing credentials. **Recommended requirements** None		**[Example]** - Wi-Fi wireless router, IP camera, medical institution system, etc. **[Reference]** **Technical standards conformity approval (Telecommunications Business Act)** **Related requirements** - Article 34 (10-4) Function to prompt change of initial state of identification code related to access control function **NIST IR8425 Related requirements** #2 Product Configuration #4 Interface Access Control **ETSI EN 303 645 Related requirements** 5.1 No universal default passwords 5.4 Securely store sensitive security parameters
1-2		New	Data Protection	**Mandatory requirements** 1) Protect information assets stored in the storage area of the device from unauthorized access and	CWE-200: Exposure of Sensitive Information to	**[Threat background]** If data protection mechanism such as encryption for the main storage, memory area, and communication is implemented

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
				modification. (The same applies to data stored in storage media such as SD cards. 2) Protect information assets transmitted to other IoT devices and servers (including cloud servers) from information leak and alteration. 3) Manage credentials (password, private key, etc.) in an area protected from unauthorized access (tampering, theft, etc.) via the network, when the device stores the credentials. **[Remarks]** For data handled as information assets, perform a risk analysis for each product/service and clarify the target information. **Recommended requirements**	an Unauthorized Actor CWE-255: Credentials Management Errors	inadequately or has some vulnerabilities, this could lead to information leakage. Regarding digital certificates used for encryption, if they are managed inadequately or have vulnerabilities, this could also lead to information leakage through data analysis. **[Example]** - Operating systems such as Windows and Linux, software modules such as OpenSSL, image viewers for medical equipment, etc. **[Reference]** **NIST IR8425 Related requirements** #3 Data Protection **ETSI EN 303 645 Related requirements** 5.4 Securely store sensitive security parameters 5.5 Communicate securely 5.8 Ensure that personal data is secure

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
				1) Implement encryption and prevent tampering data. Encryption algorithms and key management methods shall conform to the guidelines shown below. 2) Protect keys and certificates used for encryption from unauthorized access and modification. **[Guidelines related to cryptography]** - "List of reference ciphers for e-government procurement (CRYPTREC)" (Last revised: March 30, 2022, CRYPTREC LS-0001-2012R7) - "Criteria for setting cryptographic strength requirements (algorithm and key length selection)" (First Edition: June 2022, CRYPTREC LS-0003-2022)		

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
				[Supplementary documents for the above guidelines] - "CRYPTREC Cryptography Guidelines (SHA-1) Revised version" (CRYPTREC GL-2001-2013R1) - "CRYPTREC Cryptographic Technology Guidelines (Lightweight Cryptography)" (CRYPTREC GL-2003-2016JP) - "Encryption key setting guidance" (CRYPTREC GL-3003-1.0) - "Encryption Key Management System Design Guidelines (Basics)" (CRYPTREC GL-3002-1.0) - "TLS cipher setting guidelines" (CRYPTREC GL-3001-3.0.1)		
1-2	1-2-1	No change	Data erasure function	**Mandatory requirements** 1) Ensure that the information configured by the user and the information obtained during use of	CWE-226: Sensitive Information in Resource Not	**[Threat background]** If functions to delete security settings, confidential information, privacy information, etc. stored in the device and

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
				the target of verification can be easily deleted. 2) Ensure that updated system software is maintained even after deleting the information. **Recommended requirements** **None**	Removed Before Reuse	its applications are not implemented, there is a possibility that confidential information, security settings, privacy information, etc. might be leaked at the time of disposal or reuse. **[Example]** - PC, USB memory, smartphone **[Reference]** **NIST IR8425 Related requirements** *No relevant requirements specified **ETSI EN 303 645 Related requirements** 5.11 Make it easy for users to delete user data
1-3		Change	Software Update	**Mandatory requirements** 1) Implement software update functionality. 2) Ensure that the software update status is maintained even after the power is turned off. 3) Have a means to confirm that the software update has been completed normally, such as	CWE-1277: Firmware Not Updateable	**[Threat background]** If a function to update software/firmware is not implemented, and a vulnerability is found in the software/firmware, the vulnerability might be exploited because it would not be fixed. **[Example]** ・Wi-Fi wireless router, IP camera, etc. **[Reference]**

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
				displaying the version after the update. 4) Regarding the update program, the applicant shall guarantee that only genuine update is applicable, without any alterations through the update process (countermeasures against alteration). **[Remarks]** Either of the following methods is applicable. The software update is: - automatically initiated; or - manually performed by maintenance personnel or privileged users who have explicit management responsibility. **Recommended requirements** 1) Have a mechanism to verify the authenticity of the update software		**Technical standards conformity approval (Telecommunications Business Act) Related requirements** - Article 34 (10-3 Software update functionality **NIST IR8425 Related requirements** #5 Software Update **ETSI EN 303 645 Related requirements** 5.3 Keep software updated 5.4 Securely store sensitive security parameters 5.7 Ensure software integrity

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
				when the target of verification installs the update (countermeasures against tampering). 2) Encrypt communication channels or encrypt data during transmission for update software (data protection). 3) Restrict anyone other than privileged users, equipment operators or maintenance personnel from executing a function that disables the software update function, if implemented. 4) Implement a function to enable and disable notification of updates.		
1-4	1-4-1	No change	Wi-Fi authentication method	**Mandatory requirements** 1) Implement the latest authentication method recommended by the Wi-Fi Alliance®.	CWE-326: Inadequate Encryption Strength	**[Threat background]** If the communication encryption protocols used in the Wi-Fi device are not the latest, encryption algorithms used are vulnerable. **[Example]**

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
				Recommended requirements None		- Wi-Fi wireless router **[Reference]** **NIST IR8425 Related requirements** #4 Interface Access Control **ETSI EN 303 645 Related requirements** 5.5 Communicate securely
1-4	1-4-2	No change	Bluetooth vulnerability countermeasures	**Mandatory requirements** 1) Implement the latest pairing method recommended by Bluetooth SIG. 2) Ensure that unnecessary Bluetooth profiles are not recognized. 3) Ensure that the target of verification is not vulnerable to Bluetooth's Blueborne vulnerability. **Recommended requirements** None	CWE-287: Improper Authentication	**[Threat background]** 1) In the specifications before Bluetooth 2.0 + EDR, you input a common number called “PIN code” into devices to be paired. In general, 4-digit numeric input such as "0000" is used in many implementations, so security can be easily breached by guessing the number. 2) If unnecessary Bluetooth profiles are implemented then it would be subject to attacks. 3) If a device has the Blueborne vulnerability, the device could possibly be taken over by the malicious actors. **[Example]**

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
						- Devices before Bluetooth 2.0+EDR - Devices that implement Bluetooth functionality and use OS versions that may potentially be vulnerable to Blueborne **[Reference]** **NIST IR8425 Related requirements** #4 Interface Access Control **ETSI EN 303 645 Related requirements** 5.6 Minimize exposed attack surfaces
1-4	1-4-3	Change	USB access control	**Mandatory requirements** 1) Appropriately control access to the USB interface and restrict access rights. **Recommended requirements** 1) Do not implement USB ports that are not necessary for the service. 2) Take measures to make the USB ports difficult to be utilized by anyone other than the person in charge of operation.	CWE-284: Improper Access Control	**[Threat background]** If unnecessary device classes are implemented, it would be subject to attacks such as malware. **[Example]** - USB-mounted devices in general **[Reference]** **NIST IR8425 Related requirements** #4 Interface Access Control **ETSI EN 303 645 Related requirements** 5.6 Minimize exposed attack surfaces

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
1-4	1-4-4	Change	Injection countermeasures	**Mandatory requirements** 1) Significant vulnerabilities such as injection via Web input have been fixed. **Recommended requirements** None	CWE-78: OS Command Injection CWE-89: SQL Injection CWE-352: Cross-Site Request Forgery (CSRF) CWE-22: Path Traversal	**[Threat background]** If injecting commands or manipulating pathnames are possible by specially crafting the user input, it might be exploited to tamper with the backend database, to execute system commands, to bypass security checks, etc. **[Example]** - Wi-Fi wireless router（CVE-2015-6319） - Wi-Fi wireless router（CVE-2014-7270） - IP camera（CVE-2017-7461） **[Reference]** **NIST IR8425 Related requirements** #4 Interface Access Control **ETSI EN 303 645 Related requirements** 5.13Validate input data
2. **Requirements for the operation of IoT devices**						
2-1		Change	Contact and security support	**Mandatory requirements** 1) Have a contact regarding product vulnerabilities, and it is open to the	No applicable CWE	**[background]** Security standards for IoT devices at home and abroad provide criteria for

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
				public. 2) Have a mechanism to provide security updates of products in a timely manner. **Recommended requirements** None		organizational system and operations of product providers. **[Reference]** **NIST IR8425 Related requirements** #8 Information and Query Reception **ETSI EN 303 645 Related requirements** 5.2 Implement a means to manage reports of vulnerabilities 5.3 Keep software updated
2-2		New	Product documentation management	**Mandatory requirements** 1) Define and manage information related to cyber security throughout the life cycle of the product, which includes recording it in documents and updating them. **Recommended requirements** None	No applicable CWE	**[background]** Security standards for IoT devices at home and abroad provide criteria for organizational system and operations of product providers. **[Reference]** **NIST IR8425 Related requirements** #7 Documentation **ETSI EN 303 645 Related requirements** *No relevant requirements specified
2-3		New	Provision of information to users	**Mandatory requirements** 1) Clearly indicate the procedure for users to use the products securely	No applicable CWE	**[background]** Security standards for IoT devices at home and abroad provide criteria for

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
				regarding configurations and/or usage that can impact cybersecurity. 2) Inform users of the content and necessity of product software updates, and the impact in case of not updating software. 3) Inform users of disclaimers for possible accidents and failures. 4) Notify the user of the support period and end-of-support policy for the relevant products and/or services. **5)** Inform users of the assumed risks of disposing of devices with data remaining in them, and how to securely dispose of devices, including data deletion. **Recommended requirements** None		organizational system and operations of product providers. **[Reference]** **NIST IR8425 Related requirements** #9 Information Dissemination #10 Product Education and Awareness **ETSI EN 303 645 Related requirements** 5.2 Implement a means to manage reports of vulnerabilities 5.3 Keep software updated 5.11 Make it easy for users to delete user data 5.12 Make installation and maintenance of devices easy
3. Requirements for auditing IoT devices						

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
3-1		New	Audit log recording	**Mandatory requirements** None **Recommended requirements** 1) Implement audit trail recording features and enable privileged users, equipment operator or maintenance personnel to access the audit trail 2) Ensure there is sufficient storage for recording audit trail. If the storage capacity for the audit trail is exceeded, take appropriate measures such as overwriting the oldest records in order. 3) Take measures to prevent unauthorized deletion or modification for recorded audit trail. **[Remarks]** - The audit trail shall be stored in	CWE-778: Insufficient Logging	**[background]** In product incident response and security audits, recorded log data (audit trails) is required for post-incident analysis and improvement consideration. Security standards for IoT devices at home and abroad also include requirements for recording logs for the purpose of recognizing the status of cybersecurity. **[Reference]** **NIST IR8425 Related requirements** #6 Cybersecurity State Awareness **ETSI EN 303 645 Related requirements** 5.2 Implement a means to manage reports of vulnerabilities 5.7 Ensure software integrity

ID	SubID	Change Type	Security Requirements		CWE-ID	Explanation (Threat backgrounds, examples)
				the target of verification itself and/or servers to control the target of verification. The necessary size of the storage shall be separately examined based on the usage of each product.		
3-1	3-1-1	New	Time management function	**Mandatory requirements** None **Recommended requirements** 1) Implement a time management function to record the date and time of a security event in the audit trail. **[Remarks]** The requirement will be satisfied in the case where the date and time of an event can be managed by either the device or the server.	No applicable CWE	**[background]** Appropriate time management of the date and time of each event is required because recording log data (audit trail) in chronological order is important for post-incident analysis. **[Reference]** **NIST IR8425 Related requirements** *No relevant requirements specified **ETSI EN 303 645 Related requirements** *No relevant requirements specified