Crosswalk of Consumer-Grade Router Cybersecurity Standards to NIST's Baseline for Consumer IoT Products

Below is a crosswalk of the NISTIR 8425 outcomes with cybersecurity requirements from four consumer-grade router cybersecurity standards:

- Broadband Forum TR-124 Issue 8 – Functional Requirements for Broadband Residential Gateway Devices [BBF]
- CableLabs Security Gateway Device Security Best Common Practices [CableLabs]
- BSI TR-03148: Secure Broadband Router - Requirements for secure Broadband Routers [BSI]
- Infocomm Media Development Authority (IMDA) Technical Specification Security Requirements for Residential Gateways [IMDA]

The first column identifies the NIST outcomes or sub-outcomes from NISTIR 8425. The second column lists the applicable requirements from the standards. The third column is a summary of observations about the standards' requirements. More information about this crosswalk can be found at our website.

NISTIR 8425 Outcome	Informative References	Observations
Asset Identification	-	-
Asset Identification 1 *All IoT product components are identifiable.*	**BBF** GEN.DESIGN.12, GEN.DESIGN.13 [MGMT.LOCAL.20], IF.LAN.WIRELESS.AP.20 **CL** OOB-011, KEY-006, OOB-007 **BSI** (3.1.2.1)	SSID is mentioned in the three standards, but in different ways as part of formulating an asset identifier. The BBF provides additional requirements around serial numbers as well as identification of model, and CL provides some requirements about cryptographic strength of logical identifiers and use of unique materials for general cryptographic functions.
Asset Identification 2 *The IoT product maintains an inventory of all IoT product components.*	-	-
Product Configuration	-	-
Product Configuration 1 *The IoT product can be securely configured.*	**BBF** MGMT.LOCAL.2 **CL** OOB-007, DE-007, MI-002, MI-010, MI-011 **BSI** (3.1.2)[3], (3.1.2)[3], (3.1.2)[4], (3.1.2.1), (3.1.2.2), (4), (4.1.1)[1], (4.1.1)[1], (4.1.1)[3], (4.1.1)[6], (4.1.1)[6], (4.1.1)[7], (4.1.2)[Table6], (4.1.2)[2], (4.2)[2], (4.2)[4], (4.3)[2], (4.3)[3], (4.4), (4.5), (4.5), (4.8), (4.8), (4.9), (4.10)[1] **IMDA** 4.2, 4.2.3, 4.4	Documents seem to stress different specific settings that must be configurable. IMDA and BSI touch on the importance of authentication prior to accessing the admin page and configuration settings. They both stress the need for strong authentication. BSI further stresses the need to provide users feedback about the strength of a passphrase chosen. BSI also stresses limiting from where (i.e., which networks) the admin interface can be accessed. CL specifies that enabling/disabling of services/ports and disabling of cipher suites shall be supported. Also recommends that configuring the hostname should be allowed. Use of secure channels and controls like inactivity timeouts for admin access is also discussed. BBF states that the router must support configuration from the PC as defined in Broadband Forum TR-064i2.

Product Configuration 2 *The IoT product's configuration can be reset to a secure default.*	**BBF** MGMT.LOCAL.10 **CL** OOB-009, DE-003, DE-004, DE-006 **BSI** (4.6) **IMDA** 4.1.1, 4.2.1, 4.2.3	All standards specify that a factory reset is required, although BBF and BSI specify that the reset be accessible via software, IMDA via physical reset, and CL doesn't specify how. BSI specifies that reset must be performed by an authenticated user. BSI and CL specify that data and settings must be deleted when a reset is performed. IMDA requirements also list a number of settings to be off by default.
Product Configuration 3 *Configuration changes made on any IoT product components are reflected throughout all IoT product components.*	-	-
Data Protection	-	-
Data Protection 1 *Data at rest is protected.*	**BBF** SEC.FIRMWARE.2 **CL** DRP-001, KEY-001, KEY-002, KEY-003, HR-003, HR-004, SB-005, OOB-002 **BSI** (4.1.1)[7] **IMDA** 4.5	Two of the 4 standards (IMDA and CL) specify that stored sensitive data should be encrypted. The same two standards require salting and hashing stored passwords. CL gets specific in discussing secure storage elements and/or tamper-resistant hardware. IMDA specifies that encryption algorithms used should be replaceable with newer algorithms. BSI only mentions the protection of exported configuration. BBF states that encryption must be supported.
Data Protection 2 *The data on the IoT product can be returned to a factory-default state.*	**CL** OOB-009 **BSI** (4.6) **IMDA** 4.2.3	Three of the 4 have a requirement related to factory resets but only the BSI mentions that they should be performed by authenticated (or authorized) users. Only two (BSI and CL) mention erasing personal data from end-users in addition to the factory reset. IMDA discusses factory reset as part of account lock-out recovery.
Data Protection 3 *Data in transit is protected.*	**BBF** MGMT.REMOTE.WEB.6, SEC.USERINTERFACE.1, SEC.FIRMWARE.1, SEC.FIRMWARE.2 **CL** OOB-003, DE-002, DE-004, DE-005, MI-001, NETS-001, NETS-003, SBOM-006 **BSI** (3.1.2.2), (3.1.2.2), (4.1.1)[1], (4.1.1)[6], (4.1.1)[6], (4.1.1)[7], (4.1.2)[2], (4.1.2)[2], (4.4), (4.10)[1] **IMDA** 4.2.2, 4.2.5	All four documents have requirements related to data protection in transit for various functions of routers. They all mention using HTTP over TLS for external communication from the router and for using device management interfaces or web portals for configuration. All mention some minimum requirement for the encryption strength being used or protocol version, but only CL mentions specifically using FIPS approved algorithms. The other three documents list minimum versions of algorithms and protocols like TLS, WPA2, or using AES encryption and suggest use of " up to date versions." Only BSI mentions encrypting and storing configuration files (or protecting anything at rest), but it only mentions that the files should be stored in an encrypted way and be password protected without specifying that it should match the earlier requirements for passwords and encryption strength. The BSI document is the only one that mentions that passwords should not be comprised of information about the router itself (like MAC address, manufacturer name, model, etc.).
Interface Access Control	-	-
Interface Access Control 1 *Access to the IoT product's interfaces is controlled.*	-	-

Interface Access Control 1a *Only necessary interfaces are readily accessible, otherwise removed or disabled.*	**BBF** MGMT.LOCAL.1, MGMT.REMOTE.WEB.1, MGMT.REMOTE.WEB.5, MGMT.REMOTE.WEB.12, MGMT.REMOTE.WEB.13, SEC.GEN.5, SEC.GEN.6, SEC.GEN.10, SEC.GEN.11, SEC.USERINTERFACE.8 **CL** HR-001, HR-002, OOB-005, MI-003, NETS-004, NETS-005, MI-011 **BSI** (3), (3), (3.1)[2], (3.1.2)[3], (3.2)[3], (4.1.1)[6], (4.1.1)[5] **IMDA** 4.2, 4.2.1	All standards emphasize the need for secure defaults, however each approached it differently. IMDA explicitly calls out services that should be disabled by default. BSI calls out specific protocols that must be used in remote configuration access. BBF calls out that only explicitly advertised services may be enabled, and that no other services may be. CL indicates disabling serial and debug ports/consoles, and optional services by default. Telnet and FTP are explicitly forbidden to be implemented or enabled. All other services or protocols and associated ports or interfaces must be configurable. Only CL calls out disabling physical ports (serial/debugging interfaces) on the device.
Interface Access Control 1b *For necessary interfaces, access controls are in place.*	**BBF** GEN.DESIGN.14, GEN.OPS.21, MGMT.LOCAL.1, MGMT.LOCAL.5, MGMT.LOCAL.11, MGMT.REMOTE.WEB.2, MGMT.REMOTE.WEB.9, IF.LAN.WIRELESS.AP.20, SEC.GEN.1, SEC.GEN.8, SEC.USERINTERFACE.2, SEC.USERINTERFACE.3, SEC.USERINTERFACE.4, SEC.USERINTERFACE.5, SEC.USERINTERFACE.6, SEC.USERINTERFACE.7, SEC.USERINTERFACE.9 **CL** OOB-001, OOB-004, OOB-006, OOB-008, OOB-010, OOB-012, MI-004, MI-007, MI-008, MI-009, MI-010, MI-013, DIAG-002, NETS-007, NETS-008, NETA-001, NETA-002, NETA-003, MI-002 **BSI** (3.1)[1,2], (3.1.2.1), (3.2)[3], (3.2)[3], (3.2)[3], (4.1.1)[1], (4.1.1)[1], (4.1.1)[2], (4.1.1)[2], (4.1.1)[5], (4.4) **IMDA** 4.1, 4.1.1, 4.1.2, 4.2, 4.2.1	All standards addressed default passwords, noting they should be unique when in the default state (or in one case, IMDA, the device should be disabled) and the user should be prompted or required to change the password. All standards also discussed password requirements with two stating password strength requirements (IMDA and BSI). BSI went further and noted that this password should be used to authenticate users for configuration purposes. BSI also notes there shall be protections against brute force attacks. BBF states a password should be used, but doesn't dictate strength requirements. BBF does note other aspects of protecting accounts, such as time out for account log in and limiting based on failed log-ins. CL also mentioned passwords, but noted they shall not be immutable and not weak. CL also calls out that Wi-Fi access point shall use customer unique credentials. BBF and CL mention support for 2FA. BBF states the firewall should not reveal closed ports on a scan and that the router shall not reply to requests over a port for an API/Protocol that doesn't use the port. CL called out WPA2 and 802.1x support for wireless and wired connections, respectively. The standard also stated that only secure protocols should be used for control and management and that “advanced architectures such as virtual interfaces” must be secured the same as applied to physical interfaces. CL also contains requirements for configurability of account session inactivity timeout. All standards also addressed, to one degree or another the limiting of access by services and connections. IMDA indicates services that should be off by default. BSI states that access should be restricted to authorized services, that minimal services should be publicly available, and that based on configuration, access to VOIP and remote configuration services should be limited. BBF includes physical provisions, including that users should not be able to access any port intended for technicians. Beyond that, the standard also states that “back door” entry must not be allowed (e.g., example given is “there must be no hidden telnet or web access using secret passwords”), LAN-side configuration shall be disabled for bridged connections, and limited admin access through remote access. CL provisions about limiting access include that public access to administration should be limited, secure management protocols should be limited to the interfaces on which they will be used, that firewalls shall only allow accepted connections, and any method of accessing the device can be enabled or disabled.

Interface Access Control 1c *Access and modification privileges are limited.*	**BBF** MGMT.REMOTE.WEB.3, MGMT.REMOTE.WEB.4, SEC.GEN.7 **CL** MI-006 **BSI** (3.1)[1,2], (3.1.2)[4], (3.2)[3], (3.2)[3], (3.2)[3] **IMDA** 4.2	IMDA states that access to the admin page and changes to configuration should be controlled. BBF requires the user be able to make temporary WAN side remote access read-only and that any such access should be read-only be default. Additionally, it is required that the password for the router cannot be changed using WAN side remote access. It also requires the application of the principle of least privilege. CL has a requirement limiting admins to one concurrent session.
Interface Access Control 2 *Access control can be maintained to IoT product interfaces.*	-	-
Interface Access Control 2a *The IoT product validate data format.*	**CL** MI-012, NETS-006 **IMDA** 4.6	Two standards address this outcome (IMDA and CL). Both require data input validation. In addition, CL requires IP packet filtering for the firewall.
Interface Access Control 2b *Prevent unauthorized transmissions or access to other product components.*	**CL** MI-005, NETS-006 **BSI** (3.1.2)[3], (3.1.2)[3], (3.1.2)[4], (4.3)[1], (4.3)[3], (4.7)[1], (4.7)[1], (4.9)[1], (4.9)[1] **IMDA** 4.2.1	Two standards (IMDA and BSI) mention the limitation of IPv6 functionality, with IMDA stating that tunneling should be off by default and BSI stating that inbound IPv6 packets should only be forwarded when they belong to a known connection, and that only certain IPv6 message types should be used. Otherwise, the standards all address different topics. IMDA lists a number of protocols and services that should be disabled by default and states that usage statistics shall not be collected. BSI states more requirements than IMDA and touches on more concepts. Configurable and Community WLAN access controls are stated. Firewall capabilities and functionalities are described. Additionally, there are two VOIP related provisions. CL states that routers shall have mitigations against brute force attacks and must support ingress and egress filtering for IP.
Interface Access Control 2c *Maintain appropriate access control during initial connection and when reestablishing connectivity.*	**BSI** (3.1.2.3), (3.2)[2] **IMDA** 4.1, 4.1.1, 4.2, 4.2.1	IMDA states requirements for initial default credentials and device behavior in the default state. Also states that only authorized personnel should be able to edit the configuration settings and that the user is protected from being unintentionally or maliciously locked out. Finally, it states that a number of protocols and services should be off by default, data and statistics should not be sent back to the manufacturer by default, firewall is on by default and support is there for NAT, and IPv6 tunneling mechanisms are off by default. BSI states that if WSC is offered, it is deactivated before initialization, and uses a PIN that is reset after initialization. Also states NFC based WPS should be deactivated before initialization. Finally, requires that after initialization the router must restrict access on the WAN interface to a defined list of services provided by the router.

Software Update	**BBF** GEN.OPS.15, GEN.OPS.24 **CL** SU-004	Provisions from two standards deal with integrity protections related to updates. CL states that integrity protections must be in place and BBF has two provisions related to integrity, one requiring the preservation of configuration settings and another requiring fallback to a usable state in case of a failed update.
Software Update 1 *The IoT product can receive, verify, and apply verified software updates.*	**BBF** GEN.OPS.22, GEN.OPS.23, **CL** KEY-004, KEY-005, SB-001, SU-001, SU-005, SBOM-009, SB-002, SU-003 **BSI** (4.2)[1], (4.2)[3], (4.2)[3], (4.2)[6] **IMDA** 4.3	Verification of updates is required by all of the standards. All four standards either imply or explicitly state that devices be updateable. BBF recommends and CL requires signing updates. BSI recommends redundant storage. CL recommends acceptance of encrypted and co-signed updates and has additional requirements about specific software components that shall (i.e., trust anchors) or should (i.e., certificates and associated key pairs) be updateable.
Software Update 2 *Measures are in place to keep software on IoT product components up to date*	**BBF** GEN.OPS.19, GEN.OPS.20, MGMT.LOCAL.15, MGMT.LOCAL.21, MGMT.LOCAL.22 **CL** SB-003, SU-002, SU-006, SBOM-003, SBOM-007, SBOM-008, SBOM-010 **BSI** (4.1.2)[Table 6], (4.2)[1], (4.2)[2] **IMDA** 4.3	IMDA and BSI recommend automatic updates with the customer also being able to perform the update manually. BSI further states that the customer should be notified when an update is available. IMDA states updates are to be verified and not contain sensitive data. BBF states updates should be available from a public location and requires the ability for the user to browse, select, designate a predefined location to find, and install updates through a web GUI. CL discusses anti-rollback and mitigations against downgrade attacks, graceful recovery from failed updates, and devices not using or accepting deprecated software/updates. Also states that the manufacturer should use the most recent software/libraries and upgrade software with known vulnerabilities in a timely manner.
Cybersecurity State Awareness	**BBF** GEN.OPS.6 **CL** AR-002	BBF discusses responding to faults. CL requires showing indicators when certain components are in use.
Cybersecurity State Awareness 1 *The IoT product securely captures and records cybersecurity state information.*	**BBF** GEN.OPS.18, LAN.FW.2, LAN.FW.3, LAN.FW.4, MGMT.LOCAL.18, MGMT.LOCAL.20 **CL** SB-004, LOG-001, LOG-002, LOG-003, LOG-004, LOG-005, SB-002, TS-001 **BSI** (4.1.2)[1], (4.1.2)[Table 6], (4.1.2)[Table 6], (4.1.2)[Table 6], (4.1.2)[Table 6], (4.1.2)[Table 6], (4.1.2)[2], (4.8)	BSI and CL are the most comprehensive on the information that the router needs to capture in cybersecurity state logs, including login attempts, administrative events, system status, firewall status, connected devices and timing synchronization. BBF is less specific about what should be logged, but has minimum sizes for logs and rules for how to handle log data that the other documents do not have and that software/firmware versions must be identifiable via the GUI. BBF also requires that updates are identifiable by version number. IMDA has requirements like handling login attempts and firewall rules that would need a logging component to function correctly. Two of the documents mention using a hardware root of trust, and the BSI document mentions providing logging information to an authenticated user.