Cybersecurity Model Similarity Declaration

Applicant: Advantech Co., Ltd.

Address: No.1, Alley 20, Lane 26, Rueiguang Road, Neihu District, Taipei 114519, Taiwan, R.O.C.

Contact Person: **Jack Hsu**

Telephone / E-mail: **886-2-7732-3399 / jack.hsu@advantech.com.tw**

Dear Sir / Madam,

We declare on our sole responsibility that all models listed in the table below behave identical in concern with the Radio Equipment Directive 2014/53/EU (RED) article 3.3 (d, e, f) essential requirements for cybersecurity.

The analysis and testing by Bureau Veritas of the representative member of the family concerning RED cybersecurity therefore is applicable also to the other product variants listed below.

Different models are only used to distinguish due to structure, circuit arrangement, form factor, commercial use (brand, housing), etc., without effecting cybersecurity features.

Family	ICR-1700 series			
Variants	**Name** **Model Number**	**Hardware Version**	**Software Version**	**Difference Recognition**
	ICR-1745W-EU-A	A	ICR-17x5-EU_x.y.z	The ICR-1745W is an industrial-grade 5GNR gateway equipped with five Ethernet ports and integrated GPS functionality (see Annex Table 1). Its configuration is independent of the network security baseline.
	ICR-1745WE-EU-A	A	ICR-17x5-EU_x.y.z	The ICR-1745WE is an industrial-grade 5GNR gateway equipped with five Ethernet ports and integrated GPS functionality (see Annex Table 1). Its configuration is independent of the network security baseline.
	ICR-1745-EU-A	A	ICR-17x5-EU_x.y.z	The ICR-1745 is an industrial-grade 5GNR gateway equipped with five Ethernet ports and integrated GPS functionality (see Annex Table 1). Its configuration is independent of the network security baseline.
	ICR-1745E-EU-A	A	ICR-17x5-EU_x.y.z	The ICR-1745E is an industrial-grade 5GNR gateway equipped with five Ethernet ports and integrated GPS functionality (see Annex Table 1). Its configuration is independent of the network security baseline.

Cybersecurity Baseline Policy		
Mechanism	**Implementation Measures**	**Description**
Access Control Mechanism	User Authentication	Use HTTPS and SSH.
	Principle of Least Privilege	1) Root: The superuser with full system privileges 2) Admin: An administrative role with elevated privileges, but restricted from performing all root-level operations. 3) User: A standard user role with limited permissions
Authentication Mechanism	Authentication Mechanism	The methods to validate the appropriateness of the access control mechanism solely rely on role-based access control. RBAC integrates with password-based authentication to verify user legitimacy.
	Password Strength	• Must be at least 8 characters long • Must have at least 2 classes (upper / lower letters, digits, other) • Must not be palindrome • Must not contain username • Must be at least 1 character different from the old password • Must not be a rotated old password • Must not be an old password with case changes only
	Anti-Brute Force	1) Limit the number of consecutive invalid access attempts by any user within a configurable time. 2) When this limit is reached, access is denied for a specified time.
Secure Update Mechanism	Software update	The equipment supports firmware upgrade and automatic firmware update via Management Interfaces.
	Automatic upgrade failure handling	When the upgrade fails, it will automatically roll back to the version before the upgrade.
	Software update management	1) For enhanced security, it is strongly recommended to regularly update your router's firmware to the latest version. 2) Avoid downgrading the firmware to a version older than the production release, and refrain from uploading firmware meant for different models, as these actions can lead to device malfunction. 3) It is advisable to update all Router Apps to their latest versions concurrently with the router's firmware.
	Clear upgrade prompt information	The release note requires presenting and explaining the updated content to users, as well as informing them of the resolved issues and business impacts.
Secure Storage Mechanism	Secure Storage Mechanism Measure	The assets are only accessible through the HTTPS/SSH, and the HTTPS/SSH uses role-based access control to ensure that only users with admin privileges can update the assets.
	Backup and Recovery	There is a firmware backup area, and if the current partition is damaged, it will be transferred to the backup partition for operation.
Secure Communication Mechanism	Encryption algorithm and parameter update mechanism	The update of encryption algorithms follows the firmware update.
	Integrity and authenticity protection	All data transmission is checked.
	Confidentiality protection	All data transmission is encrypted.
	Replay protection	Secure communication mechanisms prevent replay attacks.
Resilience Mechanism	Anti-DoS attack	Firewall mechanisms can mitigate the impact of DoS attacks on network interfaces by filtering excessive traffic and enforcing rate limits. After an attack, the system can recover to a defined state through various resilience mechanisms such as connection timeouts, resource reallocation, and interface reset policies.
	Network disconnection recovery mechanism	Support VRRP and Backup Routes to maintain network connectivity in the event of a disconnection.
Network Monitoring Mechanism	Real time monitoring	iptables provides monitoring mechanisms to inspect and analyze traffic passing through all network interfaces.
	Detection of ICMP or ARP	Support ARP and ICMP protocol monitoring, which can be used to prevent DoS attacks.

Traffic Control Mechanism	Traffic Control Mechanism	iptables control whether network traffic is allowed by evaluating packet headers and enforcing predefined rules, ensuring only legitimate traffic is accepted.
General Equipment Capabilities	Vulnerability Management	The latest firmware requires regular vulnerability scanning.
	Principle of Minimal Services	The device starts only essential services upon boot-up, while all unnecessary services remain disabled by default.
	Input data validation	Verification and testing are available
	Restore factory settings	Users can only restore factory settings through the reset button. Once the factory settings are restored, all sensitive information is cleared.
	Risk Assessment	Followed Advantech cybersecurity policy.
Cryptography	Best Encryption Practices	The device adopts the best encryption practices for protecting security assets or network assets.

Annex Table 1

Model	Micro SIM Slot	eSIM	5 x Gigabit Ethernet	5GNR Modem	1 × RS232 1 × RS485 1 × DI 1 × DO	GNSS	Wi-Fi 6 2T2R
ICR-1745W-EU-A	x2		✓	✓	✓	✓	✓
ICR-1745WE-EU-A	x1	✓	✓	✓	✓	✓	✓
ICR-1745-EU-A	x2		✓	✓	✓	✓	
ICR-1745E-EU-A	x1	✓	✓	✓	✓	✓	

Sincerely yours,

Signature: Jack Hsu

Title: Senior Manager

Company Name: Advantech Co., Ltd.

Date: 2025/11/19