Service Addendum CYBRNC: Additional Terms for CSA Group Cybersecurity Non-Certification Services ("Cybersecurity Terms")

1. General

1.1 These Cybersecurity Terms are in addition to the Global Service Agreement ("**GSA**") and apply to all non-certification cybersecurity services ("**Cybersecurity Services**"), provided to you by CSA Group Testing & Certification Inc., whether directly or indirectly through subsidiaries, corporate affiliates or authorized third party contractors throughout the world (collectively referred to as "**we**", "**us**", "**our**" or "**CSA Group**"). The term "**Facilities**" has the same meaning as used in the GSA.

1.2 Cybersecurity Services consist of our evaluation of a limited number of your network-connectable product, aspects of a product, or system (your **"Tested Product")**, to specific requirements, and upon completion, delivery to you of a written final report with findings and recommendations regarding your Tested Product. Cybersecurity Services may include one or more of the following:

1.2.1 Gap Analysis and Risk Assessment Service: Your Information Security Management System (ISMS) and Security Development Lifecycle (SDLC) is evaluated to identify strengths, weaknesses, procedural and policy changes that should be undertaken in order to support a secure SDLC process and demonstrate that your company has performed exhaustive due diligence for mitigating security risk.

1.2.2 Vulnerability Identification Testing: We define and detect the security weaknesses of your system or product and forecast the effectiveness of proposed features and countermeasures and evaluate their actual effectiveness after they are put into use. These security weaknesses are analyzed for their impact on the functional security requirements applicable at the security level to which the device or product is designed.

1.2.3 Penetration Testing: Assess the security of your connected system by trying to exploit its vulnerabilities in a non-intrusive manner. Through this purposeful internal testing of a system, network or software, your company can help assure the security of information systems and services, so that security weaknesses can be corrected before they are exposed to attack. Our penetration tests are designed to achieve a specific, attacker-simulated objective and provide findings of how security was breached in order to reach the agreed-upon safety goal.

1.2.4 Communication Robustness Testing: Examine product resilience when subjected to network stress testing to identify network-based security vulnerabilities. We identify the presence of common programming errors and known denial-of-service (DoS) vulnerabilities which impact the robustness of embedded devices that use those networking protocols.

1.2.5 Other Testing. Performance of other tests we deem necessary to determine whether a representative product sample conforms to the applicable requirements.

1.3 Certification services. Certification services involving our evaluation of products that you intend to manufacture on an ongoing basis, to specific requirements in a standard published by a recognized standards development organization, and which may include a license of our certification mark, are specifically excluded from these Cybersecurity Services and are outside the scope of this **Service Addendum CYBR**. Cybersecurity certification services are subject to **Service Addendum NACT: Additional Terms for CSA Group Certification Services – North America**.

1.4 Compliance with these Cybersecurity Terms is a condition of our Cybersecurity Services to you.

1.5 The scope of our Cybersecurity Services is defined by you. You shall provide us with all applicable requirements, specifications, protocols and/or penetration tests that we are to use in performing the Cybersecurity Services, as stated in the relevant written quotation (the "**Cybersecurity Requirements**") for a particular version or configuration of your Tested Product. You are solely responsible for developing or sourcing from third parties all of the Cybersecurity Requirements, as well as obtaining necessary permissions from third party hosted servers or services, and shall be responsible for the content of the Cybersecurity Requirements regardless of the source of information used in their development. You must comply with the Cybersecurity Requirements at all times, including any changes to the Cybersecurity Requirements as determined by us in our sole discretion. You consent to the receipt of newsletters, Informs, or other types of notices that communicate industry changes to Cybersecurity Requirements, and you will furnish proof of compliance with such changes to Cybersecurity Requirements in the form required by us.

1.6 You warrant that each Tested Product that we have evaluated under these Cybersecurity Terms, produced or manufactured, regardless of branding or designation, is consistent in construction to the sample submitted to us and meets the Cybersecurity Requirements. You are responsible for ensuring that ongoing production of a Tested Product continues to fulfill the Cybersecurity Requirements.

1.7 You may not use cybersecurity test reports delivered by us in such a manner as to bring CSA Group into disrepute or make any written or verbal statement regarding the cybersecurity services that we have performed for any of your products unless authorized in writing by us, nor make any statements that we may consider misleading or unauthorized.

1.8 For some Cybersecurity Services, CSA Group will publicly list your name, business address and identification of the Tested Product, and you consent to such listing.

1.9 You must provide and maintain with us a current list of all unique model identifiers and brands under which your Tested Product may be distributed. You are responsible for notifying other brand owners of changes affecting a Tested Product.

2. Cybersecurity Services and Fees

You will pay the following fees to us. We may revise our fees from time to time, and unless you exercise your right to terminate these Cybersecurity Terms, you will pay the revised fees.

2.1 Testing and evaluation service fees;

2.2 All inspection fees, and costs associated with inspections, including inspections conducted after the suspension, withdrawal or cancellation of a final test report, or a Tested Product, or termination of these Cybersecurity Terms. We are entitled to set off fees for post-cancellation or similar inspections against prepaid inspection fees, if any;

2.3 Multiple listing fees if you wish to market or merchandise a Tested Product under different brand names;

2.4 Assessment fees if we determine that assessments of Facilities and/or operations are required as a result of Your Change (as defined in section 7.1);

2.5 Re-evaluation fees if we determine that samples must be submitted to us as a result of changes to the Cybersecurity Requirements or construction or design of Tested Products;
2.6 Investigation, inspection or audit fees if you are in default of any of your obligations under these Cybersecurity Terms and/or if corrective action is required to ensure that your product is compliant with the Cybersecurity Requirements;
2.7 Administrative fees for removing models from our product listing, including as a result of termination of the GSA or these Cybersecurity Terms; and
2.8 Applicable sales taxes, surcharges, and customs brokerage fees.

3. Scope; Limitations and Exclusions.
Cybersecurity Services do not alleviate your sole responsibility for: (a) product design, product functions or functional testing; or (b) the manufacture, installation, maintenance, use or misuse of your product, whether standalone, integrated or otherwise in combination with any other product or service. Cybersecurity Services do not detect or identify any vulnerabilities or weaknesses that may arise from the exposure of your Tested Product to physical damage or loss, destruction, tampering, or extreme operating environments.

4. Model Numbers
For each Tested Product, you must furnish each product model with a distinctive means of identification, which may include a model designation, catalogue number, series or type number. This means of identification must be distinctly different, in our opinion, from identification used on: (i) similar products untested by us; and (ii) recalled or discontinued products.

5. Third Party Tools and Documentation.
Cybersecurity Services may include our use of programs, documentation and tools provided by third party vendors. Those programs, documentation and tools may result in reports, data or other materials related to the Tested Product, and we retain sole ownership and control of the reports, data and other materials, except to the extent delivered in our written final report to you. You are prohibited from distributing such reports, data or other materials to third parties without our prior written consent, but you may distribute an unaltered version of our final written report.

6. Your Role and Obligations.
6.1 In addition to providing us with your Cybersecurity Requirements, your role and obligations towards the successful completion of Cybersecurity Services may include one or more of the following:
a) You will provide to us your intended use and all documented configurations, specifications, processes, procedures, or other reasonable information requested by us that is related to the Tested Product.
b) You will provide to us all requested feedback, response to additional information requests and reasonable technical support.
c) You will back up all data, programs or other files before Cybersecurity Services begin, and you acknowledge, accept and hold harmless CSA Group from all liability for any loss of data or business interruption that may result from the Cybersecurity Services.

7. Notice of Material Changes
7.1 You must inform us immediately of any changes that may affect your ability to conform with Cybersecurity Requirements, including without limitation changes to legal, commercial, organizational status or ownership; key managerial, decision-making or technical staff; modifications to the Tested Product or production method; changes to the Cybersecurity Requirements; change of your contact address and production sites; scope of operations in the production method; major changes to the management system; or relevant changes to your quality system ("**Your Change**").
7.2 Without limitation to the above, you must provide us with at least ninety (90) days' prior written notice of any changes to: name, address, or your owner; name, address or ownership of Facilities where your Tested Product is manufactured and/or any changes to brands or designations under which a Tested Product may be distributed. You will provide proof of any such changes in the form required by us.

8. Advertising
8.1 For Cybersecurity Services only, upon receiving final written test reports from us for your network connectible products, and only while the GSA and these Cybersecurity Terms are in force, you may refer to such products as "Tested by CSA", but otherwise you may not use or reproduce our name, trademarks, or state or imply that we have approved, endorsed, or certified your products or any aspects of your products.
8.2 Any claims made by you must not mislead the public.
8.3 At our request, you will amend or discontinue all advertising, promotion or other activity deemed inappropriate by us, all at your own expense. This obligation requires you to instruct third parties acting at your direction.

9. Disclaimers and Indemnification.
9.1 Supplemental to those disclaimers and indemnification described in the GSA, you acknowledge and agree to the following:
a) Cybersecurity Services are not a substitute for your own design, manufacture, test, sale or distribution, warranty and support of your Tested Product or its network connected products and systems.
b) Cybersecurity Services may not detect or identify all errors, flaws, vulnerabilities or weaknesses in a Tested Product or related software or systems.
c) Cybersecurity Services may cause the Tested Product or its network connected products and systems to fail, error out or become unavailable.
d) Cybersecurity Services do not create or result in any representation or warranty as to the security of the Tested Product or its network connected products and systems, nor the susceptibility to withstand external attacks, hacks, or breach.

e) Cybersecurity Services do not create or result in any liability attributable to programs, documentation and tools from third-party vendors or CSA Group.
f) Cybersecurity Services are subject to and contingent upon your ability to obtain penetration testing permissions from applicable third parties.

10. Complaints, Incidents and Corrective Action

10.1 You must keep a record of all complaints made known to you relating to compliance with Cybersecurity Requirements and must make these records available to us upon request.
10.2 You must notify us immediately of any reports or incidents (including those within your organization) of security breach, compromise, vulnerability, physical injury, property damage, or potential hazards that involve the Tested Product.
10.3 We may investigate complaints, reports and incidents relating to Tested Product. You must cooperate with our investigations and, if applicable, you will undertake such corrective action as required by us, at your expense, to ensure that the Tested Product is brought into compliance with the Cybersecurity Requirements, or as otherwise required to address any potential hazards.
10.4 Without limiting the above, you must take appropriate action with respect to complaints and deficiencies relating to Tested Product that affect compliance with Cybersecurity Requirements. You must immediately notify us of any pending recalls or other corrective action. You must document and maintain records of the corrective action and provide such records to us immediately upon request.
10.5 For a Tested Product, you will undertake such corrective action as required by us to address any potential hazards.

11. Term, Termination, Cancellation, and Survival

11.1These Cybersecurity Terms remain in effect until terminated by either party upon thirty (30) days' written notice to the other party, or termination of the GSA, whichever first occurs.
11.2 We may suspend, withdraw or cancel a final test report, or a Tested Product, or terminate these Cybersecurity Terms upon thirty (30) days' prior written notice. Upon such suspension, withdrawal or cancellation, or upon termination of these Cybersecurity Terms, you agree to immediately: discontinue the use of any advertising or public representations referencing applicable product(s) or services; return all applicable cybersecurity documents and CSA Group Intellectual Property (as defined in the GSA); and take any other measure requested by us.
11.3 We will not be liable for direct, indirect, incidental, consequential or punitive damages, including damages for financial or economic loss arising out of suspension, withdrawal or cancellation of a final test report, or a Tested Product, or for termination of the GSA or these Cybersecurity Terms.
11.4These Cybersecurity Terms will remain in force for any final test report or Tested Product not affected by the suspension, withdrawal, or cancellation.

