

Supplier Requirements:

Capitalized terms not otherwise defined herein shall have the meanings ascribed to them in the Agreement and SOW.

1. Worldwide Compliance Standards

The following are product specific compliance specifications for the Cisco Project and are in addition to the requirements set forth in the compliance related section(s) of the Agreement, which could be entitled "Compliance with Laws/Policies". Without limiting the requirements set forth therein, Supplier also agrees that the Product shall comply with the requirements listed in this section.

1.1. Compliance with Laws/Policies

a. General Compliance

Supplier represents and warrants that it has complied and shall comply with all applicable laws, regulations, and other governmental requirements in effect at the time of development and/or manufacture of each of the Products, in the location where the products are manufactured, as well as in the locations where the products will be distributed, sold, and used, as identified by Cisco below. Cisco may, upon request, require Supplier to provide documentation certifying compliance with any of the applicable laws, regulations or governmental requirements that are applicable to the Product, Deliverables or services being furnished hereunder. Supplier shall comply with Cisco's materials content requirements as provided to Supplier from time to time and shall undertake testing sufficient to validate compliance with such requirements. Supplier shall diligently pursue effecting its operations and performance hereunder in accordance with Cisco's Supplier Code of Conduct as published at Cisco.com and updated from time to time. Supplier shall promote Cisco's supplier diversity goals by including suppliers, where warranted, that qualify as diverse suppliers in any one or more of the categories identified on Cisco's Supplier Diversity Business Development Website www.cisco.com/supplier/diversity and as further defined at: <http://www.cisco.com/supplier/diversity/definitions.html>. Supplier shall provide to Cisco quarterly reports of Supplier's expenditures with such diverse suppliers.

b. Continuing Compliance

Supplier shall ensure that the Products continue to comply with the essential requirements against which compliance was originally declared. Any hardware/component changes to the Product may require re-testing, or in some instances re-certification of the Product. Testing must be done at an accredited testing facility, and the purpose is to verify compliance to the essential regulatory requirements, or other relevant specifications. Supplier shall bear any costs associated with laboratory testing, including without limitation any costs and expenses for third party lab or testing facilities, for continuing compliance. Notwithstanding the foregoing, if re-testing or re-certification is required due to defects in design provided by Cisco or third party, Cisco and Supplier may negotiate in good faith for Supplier to provide such re-testing or re-certification to Cisco at Cisco's cost and expense.

Continuing Compliance includes, but is not limited to, the following activities:

- Ensure that no hardware changes to the Product affect the certification.
- Review the existing Compliance Folder.
- Review the ECO's and check if these raise continuing compliance issues.
- Manage all continuing compliance queries and correspondence with surveillance authorities.

In addition to the compliance requirements set forth above and elsewhere in the Agreement, the following shall apply:

- Cisco has provided Supplier a list of countries (the "Identified Countries") where the Products will be distributed. The list of Identified Countries may be updated by Cisco from time to time.
- Supplier will design and manufacture the Products in full compliance with the laws of the Identified Countries affecting Product design, manufacture, importation, distribution and use of the Products within such countries.

Without limiting the generality of the above, Supplier is required to:

- Identify the requirements for importation and distribution/sales of the Products in the Identified Countries, and provide such information to Cisco (together with updates as any requirements may change);
- Design the Products to comply with the above-referenced importation and distribution/sales of the Products in the Identified Countries;
- Obtain any required Certifications from the appropriate authorities necessary for the import and distribution/sale of the Products in each of the Identified Countries, and provide such Certifications, with all supporting documents and information, to Cisco;
- Maintain the Certifications for the Products for each of the Identified Countries (as well as any Identified Countries newly added by Cisco), so that in the event of any change in the certification requirements or any change in the Products, Supplier will take such actions as necessary to cause the Products to remain in compliance (and provide Cisco all such updated Certifications together with all supporting documents and information).

c. Cost of redesign due to noncompliance

The payment amount payable to Supplier includes the requirement to comply with the laws, as described above, including any Identified Countries newly added by Cisco from time to time. If Supplier fails to comply with the above requirements, Supplier will, in addition to any other penalties, be responsible for Cisco's costs resulting from redesign of the Products so that it complies with the above requirements, as well as any penalties payable to the relevant government entities to obtain and/or maintain certification.

d. Custom Trade Partnership Against Terrorism

Cisco is a participant in CTPAT. For those partners who are eligible for CTPAT certification, Cisco requires documentation evidencing their CTPAT status. Cisco requires all of its partners to comply with CTPAT security criteria and provide a written statement demonstrating their compliance with CTPAT security criteria or an equivalent World Customs Organization (WCO) accredited security program administered by a foreign customs authority. Detailed information on CTPAT can be found on the U.S. Customs and Border Protection website (<https://www.cbp.gov/border-security/ports-entry/cargo-security/CTPAT>).

Notwithstanding the foregoing, if Cisco participates in or is required to participate in other similar customs supply chain security programs, Supplier agrees to comply with applicable criteria and requirements of such programs, based on mutually agreed time frames.

e. Cisco Anti-Corruption Policy

Supplier agrees to act consistently with Cisco's global anti-corruption policy posted at http://www.cisco.com/legal/anti_corruption.html at all times.

f. Scrap and Supply Chain Visibility

Supplier shall comply with Cisco's Scrap Policy and Supply Chain Visibility Policy as communicated to Supplier from time to time.

Product compliance addresses the various regulatory requirements that Cisco products must meet in order to be shipped or installed in the target markets listed in each SOW. These requirements also provide the internal design verification testing processes necessary to ensure consistent quality and reliability.

1.2. Safety Testing

The applicable Safety requirements for the Project are those for the targeted countries/regions identified in the External Technical Requirements Document ("ETRD").

Supplier will do all safety pre-testing of the Products. Supplier will obtain the necessary safety certifications to allow the Products to be shipped to targeted countries/regions.

1.3. Product Safety Standards

The Product will comply with Information Technology Equipment safety standards listed in the ETRD. Compliance to additional standards is required for Products intended for special installation environment such as hazardous locations, industrial control, and medical.

1.4. Energy Efficiency

The Product will comply with energy efficiency standards listed in the ETRD.

1.5. Cisco Product Environmental Requirements

Supplier shall adhere to the following:

Supplier acknowledges that (i) it has received a copy of Cisco's Controlled Substance Specifications, the Compliance Specification for Batteries and Products Containing Batteries and Cisco Environmental Packaging Specification (collectively, the "Environmental Specifications") as shown in Cisco's Electronic Document Control System document numbers 661823, 627058 and 886022 respectively (collectively the "EDCS Documents"), (ii) the Environmental Specifications may be updated by Cisco from time to time as set forth in the EDCS Documents and (iii) it has on-line access to the EDCS Documents, including any revisions thereto. Supplier represents and warrants that (i) it has complied fully and shall comply fully at all times while providing the Products, Deliverables or services pursuant to this SOW with the Environmental Specifications, including any updates or revisions by Cisco thereto and (ii) any information that Supplier provides with regard or in response to the Environmental Specifications, including without limitation, any certifications, acknowledgements or comparable forms, shall be complete, current and accurate.

1.6. Accessibility

Accessibility must be considered in all products being developed for or by Cisco. The Accessibility Laws that must be scoped are US Section 255 of the Telecommunications Act and US Section 508 of the Rehabilitation Act. In addition, Cisco has adopted the following guidelines as requirements for Web-Bases products: W3C Web Content Accessibility Guidelines 2.0 Level A.

2. Manufacturing Requirements

2.1. Manufacturing Core Requirements

In addition to the Manufacturing Core Requirements set forth in the Agreement, Supplier shall comply with the requirements of Cisco document number EDCS-565066, *Manufacturing Core Requirements for ODM/JDM Products*, as updated from time to time.

2.2. Manufacturing Documentation

Supplier will draft and provide the following documents to Cisco for review and approval upon request:

- i. Capacity Plans – which include manufacturing build and test capacity plans.
- ii. Yield Analysis with Root Cause Analysis and Corrective Action Plan Reports

2.3. Weekly Manufacturing Joint Development Meeting

2.4. Supplier shall present Product build readiness prior to each prototype, pre-pilot, and pilot start, which should cover Supplier's material preparation, tooling, and testing.

2.5. Sustaining Mechanical Tooling

Subject to its written pre-approval, Cisco agrees to fund the first set of production mechanical tooling (which shall be used by Supplier only for the production of Cisco products) based on volume estimates included in the Request for Quotation ("RFQ").

Supplier will be responsible and liable for the purchase, installation, and operation of any and all additional tools needed to meet production volumes. Additionally, Supplier will be solely responsible for the replacement of damaged/worn-out tools, and capacity increases based on Cisco's demand forecast inclusive of tools unique to Cisco's product manufacturing/test.

Supplier is responsible and liable for the proper maintenance and care of all tools (including those initially purchased by Cisco) to ensure high manufacturing and quality related production yields at designed run rates.

2.6. FCS (First Customer Ship)

First Customer Ship Product is "real" Product. All aspects of the production process should be controlled. International Organization for Standardization ("ISO"), Underwriters Laboratories ("UL"), Federal Communications Commission ("FCC"), and other process mandating requirements shall be observed.

2.7. Manufacturing Test

The Manufacturing Technical Requirement Document ("mTRD") will explain the detailed technical requirements for testing the Product.

From the first prototype builds through end of life ("EOL") of the Product, Supplier will provide all necessary test equipment and resources in order to meet the mTRD. Any costs beyond the requirements stated in the mTRD will be negotiated between the parties and formalized in the SOW or associated Change Request.

2.8. Manufacturing Quality

Supplier shall provide Cisco with the process Supplier uses to qualify components and to track the quality of those components throughout the production life of the Product.

Supplier shall measure structural and functional test yields at the Printed Circuit Board ("PCB") level and system test yields, either first pass yields and/or final pass yields. Supplier shall track these structural and end to end functional test yields to product specific goals. Supplier shall execute a continuous improvement process aimed at improving factory test yields and reducing visual/mechanical defects. The continuous improvement process may include but is not limited to a cross-functional team meeting on a regular basis to focus on defect reduction, track investigation improvement and/or continuous improvement actions and results, and utilize a variety of analysis tools (i.e., Paretos, trend charts, etc.) looking for root cause of issue and systemic issues. Supplier shall provide Cisco with a monthly report demonstrating continuous improvement made in the factory.

The following includes, but is not limited to, circumstances when Supplier shall provide Cisco with its yield and performance to goal data.

- a) Cisco audit
- b) High fallout in Supplier factory
- c) Field or Cisco customer escalation

d) Cisco business review

Supplier shall perform an outgoing quality audit (“OQA”) and ongoing reliability (quality) monitoring (“OQM”) on each of the Products during manufacturing, including monitoring the failure rate of both the OQA and OQM processes. Supplier shall provide a monthly report tracking monthly OQA and OQM fallout, root cause of all the failures, and the corresponding corrective action plans and progress to Cisco. If the monthly OQA failure rate is greater than 2.5% or if there are any failures during an OQM test, Supplier shall communicate these events to Cisco within one week of the failure trend or failures. Additionally, Supplier shall provide a post-mortem report within one week of the excursion that includes containment, root cause, and corrective action plans and statuses.