

OLYDEFENCE Procurement Enquiry Guide

How authorised institutional buyers should prepare a reviewable requirement

Document code	OLYD-PUB-PEG-001	Version / effective date	3.0 / 2 August 2026
Classification	Public / business review	Document owner	OLYDEFENCE — OLYVENRA LTD
Language	English	Status	Publication-ready / controlled master
Purpose			
A practical public guide to the information needed for initial fit, authority, compliance and evidence review.			

1. Establish authority

Provide the legal organisation, public or corporate mandate, authorised contact and procurement route. Identify the contracting entity and confirm the basis on which you may represent the buyer or end user.

2. Describe the requirement safely

Use generic, non-sensitive product-family, user, environment, quantity, delivery and lifecycle criteria. Do not include classified information, detailed weapon configuration, controlled drawings, encryption parameters, credentials or personal documents.

3. Identify parties and destination

Identify the buyer, consignee/importer, final end user, destination, intermediaries and anticipated transit countries. Explain the intended end use, custody and storage concept and any re-transfer constraints.

4. State the evidence required

Define the exact standard/test edition, acceptance authority, environmental or compatibility conditions, traceability, labelling/instructions, shelf/service life, warranty, training, maintenance, spares and documentation required.

5. Allocate approvals and logistics

Identify who owns classification, licences/permits, sanctions review, dangerous-goods obligations, import/customs, transport security, receiving inspection, asset records and disposal.

6. Use the controlled forms

Submit the Controlled Buyer Requirement Form for detailed requirements. If confidential information may be needed, use the NDA & Controlled Information Request Form to define scope before disclosure.

What happens next

Initial review may result in a request for clarification, evidence, enhanced due diligence, competent-authority confirmation or secure data-room access. Submission does not confirm availability, approval, licensing or a commitment to transact.

Eight gates before a controlled requirement can progress.

The following evidence is requested proportionately to product risk, destination, customer and transaction stage. OLYDEFENCE does not claim licences, certifications or approvals that have not been verified for the exact scope.

- 1. Legal identity & authority** - Legal name, registration, beneficial ownership, public authority or mandate, authorised signatory and procurement route.
- 2. Parties, destination & sanctions** - Buyer, consignee, end user, intermediaries, countries, transit route, ownership/control and applicable sanctions or embargo checks.
- 3. End use & anti-diversion** - Documented intended use, final location, custody, storage, no unauthorised re-transfer and escalation of diversion indicators.
- 4. Classification & licensing** - Military, dual-use, firearms, dangerous-goods, medical-device, PPE or other classification and the responsible licence holders.
- 5. Product identity & evidence** - Legal manufacturer, model/configuration, part number, serial or lot, current specifications, reports, certificates, labels and instructions.

6. Quality & configuration control - Quality-system scope, inspection/acceptance plan, nonconformance, change notification, authorised substitution and record retention.

7. Logistics & lifecycle - Packaging, transport, storage, shelf/service life, spares, calibration, training, maintenance, warranty, recall and disposal.

8. Human rights, IHL & secure data - Risk-based human-rights/IHL review, responsible business conduct, need-to-know access and protection of controlled technical information.

Do not send classified, export-controlled, operationally sensitive or personal medical information through the public form. Product-specific technical data, pricing, stock, licences, end-user records and contracts are shared only after due diligence through an approved channel.

Portfolio governance: configuration, origin, availability, evidence, licensing, end user, end use and support scope are validated for each authorised requirement before supplier engagement or technical release.