

OLYDEFENCE Supplier & Partner Pack

Qualification expectations for controlled defence and security supply

Document code	OLYD-PUB-SPP-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 public onboarding guide for manufacturers, authorised suppliers, integrators, maintainers, laboratories and specialist service partners.			

Who should engage

Legal manufacturers and verified production sites; authorised representatives, distributors and exporters; integrators and approved maintenance organisations; accredited laboratories; qualified logistics, training and lifecycle partners. Unidentified intermediaries, unverifiable mandates, requests to conceal parties or destination, unexplained third-party payments and attempts to bypass licensing or end-use controls are not acceptable.

Initial qualification evidence

- Legal identity, ownership/beneficial ownership, directors, registered sites, tax status and authorised signatories.
- Role and product scope, OEM appointment or provenance, licences, registrations, authorised territories and critical subcontractors.
- Quality-system scope, product/configuration controls, laboratories, inspection/release authority, nonconformance and corrective action.
- Serial/lot genealogy, counterfeit avoidance, change notification, complaint/incident/recall process and record retention.
- Sanctions, anti-bribery, intermediary-fee, human-rights/IHL, labour, HSE, dangerous-goods and information-security controls.
- Insurance, references, financial standing, service capability and lifecycle support evidence.

Product evidence package

- Legal manufacturer, production location, exact model/configuration and part number.
- Current specification, controlled drawing or data sheet, label and instructions appropriate to the destination.
- Configuration-specific test, conformity, approval or acceptance evidence with issuer, scope, revision and date.
- Serial/lot structure, certificate/release record, shelf/service-life data, packaging and storage conditions.
- Warranty, inspection, calibration, maintenance, spares, training, obsolescence and disposal arrangements.

Continuing obligations

Notify OLYDEFENCE before material changes to ownership, licence, manufacturer, site, product configuration, evidence, sanctions exposure, subcontractors or banking arrangements.

Preserve audit-ready records and support clarification, enhanced due diligence, customer inspection, corrective action and post-delivery assurance where contractually required.

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.