VEDYA PARTNERS & ADVISORS

X15, First floor, Hauz Khas
New Delhi – 110 016

Tel: +91 11 4575 6872
+91 11 4382 9908
vedyapartners.com

Security Manual for Licensed Defence Industries ('SMLDI')

1 August 2025

Overview and objectives

- It's a comprehensive regulatory framework issued by the Ministry of Defence to ensure that all DPIIT-licensed defense manufacturers implement robust security protocols before starting production.
- To safeguard classified information and materials released to licensed companies, including information released during all phases of the contracting, bidding, negotiation, performance, and termination.
- Appointment of Cyber Information Security Officer ('CISO') and Chief Security Officer ('CCSO').
- Installation of biometric access systems, watch towers, and perimeter security.
- Cybersecurity audits by CERT-IN (Indian Computer Emergency Response Team) empaneled agencies.
- Secure handling of classified documents, materials, and equipment.
- Guidelines for foreign visits, subcontracting, and international transfers of sensitive data.

Classification of sensitive items

- Category A – Products that are highly classified and sensitive and the manufacturing of these items would require the highest level of security. For example, arms, ammunitions, explosives, propellants, propulsion, aircrafts, warships, battle tanks, radars, weapons, software.
- Category B – Semi-finished products, sub-assemblies, sub-systems of main weapons / equipment / platforms and some finished products of lesser degree of sensitivity. For example, wing assemblies, structural assemblies, avionics.

Applicability

- The Manual is applicable to all companies who have been granted an Industrial License and are engaged in the production of defence products.
- When a licensed company is executing a Government project, dealing with classified information and material, it will be responsible to earmark the areas as classified, depending upon the nature of work being carried out.
- Applies to all departments handling classified materials, IT systems, and physical security.
- SMLDI covers the following aspects:
  - General provisions and responsibilities
  - Organizational security and personnel
  - Security of premises and physical security measures
  - Material security
  - Handling of documents and equipment
  - Communication

- Cyber security
- Subcontracts
- International security
- Visits and trainings

SMLDI requirement	Industrial licensing linkage	Cybersecurity audit alignment
Appointment of CCSO and CISO	Mandatory for license activation under DPIIT norms	Evaluated during CERT-IN empanelled audit for role clarity and reporting structure
Physical security (watch towers, access)	Required before production start; part of site inspection	Assessed for perimeter integrity, access control logs, and surveillance coverage
Cybersecurity posture (ISO 27001)	Must be declared in license application	Audited for compliance with ISO 27001 controls and integration with Defence CSOC
Document and material handling	Classified handling protocols must be in place	Auditors verify secure storage, transmission logs, and destruction procedures
Subcontracting and consultant engagement	Licensee must declare subcontractors and ensure NDA compliance	Audited for third-party access controls, data sharing protocols, and audit trails
International transfers and foreign visits	Requires prior approval and documentation under SMLDI	Auditors check for travel logs, visitor access records, and classified data movement procedures
Internal and external security audits	Compliance statement submitted to DPIIT	CERT-IN audit includes review of past audit reports, remediation actions, and audit readiness
Cybersecurity training	Part of organizational readiness for license activation	Auditors assess training records, phishing simulations, and awareness campaigns

Organizational security and personnel

- Licensed companies to appoint an Indian citizen as the CCSO, the CCSO should be an ex-Indian armed forces officer who with adequate knowledge of security.
- The CCSO will be positively vetted by agencies of Government before hiring and after every three years. The CCSO will be responsible for framing internal security policies, training, upgradation, and liaison with other departments and intelligence agencies of Centre and State.
- Licensed companies to appoint a CISO who will be vetted by agencies of Government and after every three years.
  - A company with more than INR 250 crore turnover, a dedicated CISO shall be appointed. The CISO will be responsible for framing and implementing cyber security policy, security audit and security training.

- Roles and responsibilities of company personnel (CEO, CCSO, CISO, CIO, Information security officer) with respect to cyber security have been specified.
- The security staff must be armed. These guards should preferably be from Defence Security Corps (DSC) / Central Industrial Security Force (CISF) / Director General Resettlement (DGR) empaneled agencies having Private Security Agencies Regulation Act (PSARA) license.
- If classified information or materials have been compromised / lost/ found in wrong place, it is to be reported to the CCSO.
- In case of possible espionage, sabotage, terrorism, and subversive activities, a report should be made to a police station, MHA and the Nodal Office. In addition, if the breach has led to data loss / compromise in cyber-security, it should be intimated to the Nodal Office, DDP.
- Personnel employed on top secret work should be subjected to prior positive vetting by Nodal Office, DDP, and then every two years. Only permanent employees shall be posted in top secret and secret sections.
- The employees of companies including those of the foreign collaborator, involved in design, development and production shall be cleared from a security angle. The list of employees cleared shall be maintained by the licensee and furnished to the Nodal Office, DDP every quarter.

Physical security of premises

- This includes securing the perimeter walls, gates, lighting, access control system of entry, protection of vital stores and designating restricted areas.
- For Category A license holder, a 10' high with 2' overhangs of punched tape, or an anti-scaling device. Under Vehicle Scanning System (UVSS) to be used for inspecting under carriage of vehicles.
- Manned guard posts or electronic surveillance with motion-detection cameras along with manned controlled rooms. Spotlights with day and night CCTV cameras with recording facility for 90 days. Guidelines issued by MeitY on CCTVs shall be strictly adhered to.
- Electric fences may be deployed along the perimeter wall.
- No construction close to the wall and minimum five meters are maintained inside the wall.
- Minimum number of gates and material gates should be different from those meant for the employees.
- A Biometric Access Control system must be installed along with a door frame metal detector, handheld metal detector, and separate frisking room for ladies.
- The administrative area should be well demarcated from the manufacturing area.
- Road barriers, speed breakers, boom barriers, etc., be employed at the gate.
- Entry of visitors to classified areas should be regulated and authorized by CEO.
- No visitor would be allowed to carry laptops, pen drives, mobile phones and any kind of storage devices or Bluetooth devices inside the premises.
- Visitors will always be escorted during their visit to the classified area.
- Official visitors from Ministry of Defence, Government of India, MHA in possession of valid id cards will also be issued with the visitor's if card at the reception office.
- Provision of weigh bridge be made at the material gate.

- Watch tower specifications have been detailed in the document.
- Day and night vision devices may be provided to the sentries based on the criticality of the installation and the assessed threat perception. Watch Towers may be equipped with dragon lights, walkie-talkie sets / intercoms and high mast light / revolving flash lights, etc.
- Personnel to carry id cards containing specified details as per the document. Vehicles to have stickers on them.
- Carriage of weapons, other than by the staff of CCSO would be strictly prohibited inside the classified area. Storage of weapons to be maintained and only authorized supervisor cadre is allowed to operate.
- In the event of emergencies like accidents, terror attacks, strikes, etc. the following procedure is to be followed:
  - Activation of control room with immediate intimation to local authorities.
  - Emergency exits / route plan to be identified.
  - Actions should be in accordance with the Disaster Management Plan.

Subcontracting

- In case of outsourcing or release of classified information to a sub-contractor provisions of security manual shall be followed. Sharing of classified material / information will be preceded by an NDA.
- Outsourcing partner's personnel and facilities would also be covered under the Official Secrets Act, 1923.
- Personnel working on such projects should be checked for character antecedents and police verification should be obtained.
- All the relevant clauses of the Manual of Security are to be made applicable for the sub-contractor.
- If classified information / material received under the subcontract is intended to be retained, the subcontractor must comply with the provisions of this manual and give an undertaking of the same Government agencies concerned.
- A licensed company should ensure that the background of the advisors / consultants are verified before hiring their services.

International security

- Where sensitive material is acquired by the licensed company, it should be ensured the equipment is securely packed and sealed and transported.
- Top secret and secret materials will not be shipped in vessels / flights which unload cargo in other countries or call at ports of unfriendly countries *en route*.
- Bills of lading or other documents will not indicate the classification of the material. Separate bills of lading may be made out for small consignments which are delivered to the Master of the Ship for personal custody during transit. These documents will not give precise details.
- Intimation will be sent to the consignee through official channels or through a coded / encrypted signal describing the equipment in general terms.

- Consignments of classified equipment awaiting shipping will be shrouded or hidden. These consignments will be adequately guarded to prevent pilferage.
- Single point contact shall be designated for the controlled movement of classified materials and documents from foreign sources with whom collaborators can communicate for secured transaction of TOT documents.
- Consignors of classified equipment will warn consignees of the classification of the equipment and the precautions to be taken.
- The names of the Government Authority of each country empowered to authorize the release and to co-ordinate the safeguarding of classified information and the channels to be used for the transfer of classified information between the participants National Security Authority (NSA) / Designated Security Authority (DSA) / Competent Security Authority (CSA) and / or Contractors involved shall be governed by an NDA.
- Consignors of top secret and secret equipment will warn the consignee of the dispatch of equipment so that the latter is able to make adequate security arrangements to receive it.