SMLDI 2025 - New Security Compliances for Defence Manufacturers in India

The Indian Ministry of Defence's (MoD) revision of the Security Manual for Licensed Defence Industries (SMLDI) in June 2025 marks a significant regulatory shift, redefining the way private sector players must operate within the country's defence manufacturing ecosystem. First published in 2014, the SMLDI has now been comprehensively overhauled in response to growing geopolitical threats, an increase in cyberattacks, and the rising complexity of the defence supply chain, especially highlighted during Operation Sindoor.

The revised SMLDI is mandatory for all entities holding a defence manufacturing license issued by the Department for Promotion of Industry and Internal Trade (DPIIT). It sets rigorous expectations across cybersecurity, physical protection, supply chain monitoring, personnel vetting, and the handling of sensitive data and documents. The aim is clear: to safeguard India's defence infrastructure by enforcing a robust and uniform security posture across all licensed industrial units.

Classified product categories and site-level obligations

The SMLDI distinguishes between:

- Category A products: Products that are highly classified and sensitive from the security angle and the manufacturing of these items would require the highest level of security. The illustrative examples of products under this category are arms, ammunitions, explosives, propellants, propulsion, aircrafts, warships, battle tanks, radars, weapons, software and various types of charges.
- Category B products: Semi-finished products, sub-assemblies, sub-systems of main weapons, equipment, platforms and some finished products of lesser degree of sensitivity such as wing assemblies, structural assemblies, barrel assemblies, turret, avionics etc.

Companies manufacturing both must either segregate facilities or uniformly implement Category A-level controls site-wide. This ensures that no weaker link exists within the production environment.

Security Leadership and Governance

Two high-level roles are now compulsory for companies:

- **The Company Chief Security Officer (CCSO)**, typically a former officer from the armed forces or police, who oversees physical security, site preparedness, staff training, and coordination with government agencies.

- **The Cyber Information Security Officer (CISO)** is responsible for developing and executing a comprehensive cybersecurity strategy, including internal audit planning, threat and vulnerability detection, crisis management and policy enforcement in alignment with agencies like the Indian Computer Emergency Response Team (CERT-IN) and the National Critical Information Infrastructure Protection Centre (NCIIPC).

Both roles are subject to stringent pre-appointment vetting and re-evaluation every three years to maintain the integrity of leadership and internal oversight.

Cybersecurity Reinforcement

SMLDI 2025 places unprecedented emphasis on cyber defence:

- Annual cybersecurity audits by CERT-In empanelled auditors are mandatory, with findings to be reported directly to the MoD.
- Multi-factor authentication (MFA), end-to-end encryption of sensitive communications, and strict compliance with national cyber directives are now baseline requirements.
- Companies must implement proactive detection mechanisms, enforce internal vulnerability scanning, and adopt clear crisis management protocols.

Enhanced Physical Security

All defence-licensed industrial units are required to:

- Establish 3-metre perimeter walls with anti-scaling measures.
- Deploy biometric access control systems (ACS) at all entry and exit points.
- Maintain 90-day CCTV footage archives for security review.
- Implement dual-level access protocols for high-security zones.
- Conduct regular emergency response drills, including intrusions, fire hazards, and armed attacks.

Employees Vetting and Training

All employees with access to classified zones /material or within sensitive areas must undergo rigorous background verification, in collaboration with law enforcement agencies, and periodic re-vetting, especially for those handling high-risk data. All staff also needs to follow a mandatory cybersecurity and physical security training. Any breach, whether intentional or accidental, triggers disciplinary actions under applicable legal frameworks including the Official Secrets Act and the Indian Penal Code.

Classified Information Handling

Access to classified information is now regulated through a five-tiered structure (TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED, and UNCLASSIFIED). These documents must be stored, marked, transmitted, and destroyed using strict procedures, with all interactions logged and formally tracked.

Control of Materials and Logistics

All inbound and outbound materials (including samples and repair tools) must be entered into digital registers or ERP/IFS systems.

Transport of sensitive items or explosives mandates armed escort, GPS tracking, transporter vetting, and local authority notifications. The transmission of classified information requires mandatory sealing, securd envelopes, and a designated supervising officer.

Subcontractor and International Coordination

The responsibilities extend beyond the primary manufacturer. All subcontractors, consultants, and international partners must conform to SMLDI norms. Visits by foreign nationals to the area, zone, manufacturing facility where the work related to MoD projects is going on are subject to prior MoD approval. International collaborations and transfer of classified information between two countries must be governed by enforceable Non-Disclosure Agreements (NDAs).

Audits, Compliance, and Internal Oversight

The SMLDI mandates that defence companies must:

1. Form a Security Council within each industrial unit to oversee internal compliance.
2. Submit quarterly compliance reports to the MoD.
3. Conduct both internal and external security audits
4. Conduct an annual Cyber audit be performed by CERT-In-accredited auditors, and results to be submitted to authorities

Conclusion

SMLDI 2025 is more than a regulatory update, it is a strategic framework to ensure India's defence industrial base is resilient, secure, and future-ready. As the bar for compliance rises, so do the expectations from private sector partners, both Indian and international. Adhering to these standards is no longer optional, it is foundational to participating in the nation's defence value chain. Licensed entities and their international partners must adapt swiftly, institutionalise robust governance structures, and view security not merely as compliance, but as a cornerstone of sovereign defence integrity.

How Baker Tilly ASA supports Defence Manufacturers

Navigating the complexities of the revised SMLDI requires more than compliance, it requires a strategic partner. At Baker Tilly ASA India, we offer an integrated suite of cybersecurity, governance and risk advisory services tailored to the defence sector's unique needs.

1 – CYBERSECURITY

Cybersecurity Audits & Compliance Management

As CERT-In empanelled auditors, we conduct comprehensive cyber audits, including ISO 27001/27701/42001 alignment, RBI/SEBI/IRDA mandate compliance assessments, and gap assessments in accordance with CERT-In and MoD expectations. We deliver detailed reports highlightinh non-compliance areas with prioritized action steps and remediation support, including policy updates and control implementation, and offer continuous compliance monitoring with periodic health checks.

Cyber Risk Assurance & Vulnerability Management

Our teams deploy Vulnerability Assessments and Penetration Testing (VAPT), red-team simulations, and application security reviews, Dark Web/ Deep Fake & Social Media monitoring to proactively detect threats and do offer take down services. We also help embed DevSecOps frameworks to strengthen security across the software development lifecycle.

Digital Forensics & Incident Response

In today's digital landscape, the threat of cyberattacks, especially ransomware, is a persistent reality for organizations of all sizes. When a breach occurs, swift and strategic response is vital. That is where a dedicated cyber incident response team steps in, offering critical support to help organizations contain the damage and restore operations effectively.

The team begins with a thorough impact assessment, identifying the root cause, entry point, and any potential lateral movement within the network. From there, they assist with removing malicious elements, cleaning infected systems, and minimizing the risk of further spread.

Regulatory requirements are also addressed with detailed reporting, while guidance is provided on cyber insurance claims to ease the post-incident recovery process. Forensic investigation and data recovery ensure organizations get back on their feet faster, with limited operational disruption.

Beyond remediation, the response team advises on preventive measures, aimed at strengthening cybersecurity posture and reducing the chances of future incidents. The goal is not just recovery, but resilience: helping organizations bounce back swiftly and with confidence, protecting both their business continuity and their reputation.

Secure Technology Integration

From IoT and cloud deployments to AI-driven controls, our experts help defence manufacturers assess and securely implement emerging technologies, ensuring resilience without compromising national security requirements.

2 – INTEGRITY DUE DILIGENCE & SUPPLY CHAIN OVERSIGHT

Employee Vetting & Insider Risk Prevention

We conduct deep background verification on employees with access to sensitive zones or classified material, including litigation checks, credit history reviews, media profiling, and ethical behaviour assessments.

Third-Party Risk & Supply Chain Oversight

We assist companies in evaluating and managing their subcontractors, vendors, and logistics partners through integrity due diligence, conflict of interest checks, reputational reviews, and legal history analysis.

Market Intelligence & Strategic Due Diligence

Leveraging discreet field investigations and corroborated intelligence gathering, we uncover hidden risks related to subcontractors, consultants, or potential JV partners to support pre-engagement decisions.

Asset Tracing & Fraud Investigations

Our forensic experts specialize in locating and assessing tangible and intangible assets, including real estate, financial securities, IP, and high-value personal property. We support investigations into asset diversion, hidden ownership structures, and fund misappropriation - key for evaluating internal fraud or vendor misconduct.

Bhushan Sharma
National Head, Risk Advisory
bhushan.sharma@bakertilly.in

Shrikrishna Dikshit
Partner, Cybersecurity
shrikrishna.dikshit@bakertilly.in

Léa Parmentier
French Desk
lea.parmentier@bakertilly.in