July 2025

Reforming defence security: Key highlights of press note 3 of 2025 and India's updated security manual

India's defence manufacturing sector is witnessing rapid growth, driven by record-high exports, strategic policy reforms, and the push for self-reliance under the Atmanirbhar Bharat initiative. With major investments, industrial corridors, and increased private sector participation, India is steadily positioning itself as a global hub for defence production and innovation.

With the objective to strengthen security guidelines for defence company, the Department for Promotion of Industry and Internal Trade has released the press note 3 of 2025 apprising that the Department of Defence Production ("**DDP**"), Ministry of Defence ("**MoD**"), has issued a revised Security Manual for Licensed Defence Industries ("**Manual**"). This revision is aimed to address the rapidly evolving security and technology landscape especially the recent surge in sophisticated cyberattacks targeting Indian defence establishments.

This marks the first significant update since the 2014 Manual ("**2014 Manual**"), which required substantial overhaul to keep pace with contemporary security and operational demands. The updated Manual places greater emphasis on cyber and physical security, risk based categorisation of industries and mandates compliance for all companies holding industrial licences issued by the DDP. It aims to safeguard classified information, materials, and infrastructure across licensed defence production sites.

The highlight of the Manual include the following:

1. **Structural overhaul:** A significant element of the Manual is the classification of products into defined categories based on sensitivity and security risks associated with each product type::

    a) Category A: 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.)

    b) Category B: Semi-finished products, sub-assemblies, sub-systems of main weapons/equipment/platforms and some finished products of lesser degree of sensitivity. The illustrative examples of products under this category are wing assemblies/structural assemblies/barrel assemblies/turret/avionics etc.

2. **Appointment of the Company Chief Security Officer ("CCSO")**:Each Indian Licensed Defense Company ("**ILDC**") or its multi-location units must appoint an Indian citizen as the CCSO who will be an ex-army/central paramilitary/police officer, responsible for ensuring that all security measures necessary for implementing the provisions of the Manual are in place. Persons of Indian Origin and Non-Resident Indians are excluded from such appointments. Any person with adverse remarks in their release certificate is also ineligible to hold the position

of CCSO. CCSO are subject to be vetted by government agencies through the nodal office, DDP, before hiring and every 3 (three) years subsequently.

3. **Appointment of the Cyber Information Security Officer ("CISO")**: The Manual significantly expands the role and requirements of the CISO compared to the 2014 Manual with the objective to enhance accountability, structural clarity, and proactive cyber risk management, aligning with modern threats and national security expectations while ensuring robust and continuous protection of critical information infrastructure across organisational levels.

   While the 2014 Manual allowed any senior officer with adequate computer knowledge to perform CISO functions alongside other duties, the Manual mandates positive vetting by government agencies before appointment and every 3 (three) years subsequently.

   Manual introduces a turnover-linked requirement for companies above INR 250,00,00,000 (Indian Rupees two hundred and fifty crore) to appoint a dedicated CISO and specifies that the officer must have the necessary and sufficient IT system knowledge. The Manual elaborates detailed responsibilities, including the implementation of cyber security controls, incident response, maintaining threat awareness, internal audits, third-party risk assessments, automated monitoring, and incorporating information security clauses into contracts.

4. **Cybersecurity framework**: The Manual marks a significant advancement over the 2014 Manual, establishing a far more comprehensive and proactive cybersecurity framework, mandates a multi-tiered governance structure, including a dedicated, government-vetted CISO and a cyber security division. Cybersecurity policies must now be comprehensive, annually reviewed, and based on expert risk assessments, with explicit ISO 27001 compliance and continual improvement processes. Technical controls have evolved from basic measures such as anti-virus and patching to advanced solutions including Zero Trust Architecture, SIEM, SOAR, MFA, and network segmentation.

   Audit and compliance requirements are more rigorous, demanding both internal and external annual audits, automated monitoring, and strict follow-up on audit findings. Incident response is now holistic, covering the full lifecycle from preparation to recovery, with mandatory root cause analysis and detailed reporting to authorities. Regular, documented training is required for all personnel, including contractors, and supply chain security is robustly addressed through vendor vetting, contractual clauses, and software provenance management.

5. **Physical security measures**: A more robust and detailed regime for physical security compared to the 2014 Manual is introduced in the Manual through a multi-layered approach to securing premises, with explicit requirements for perimeter security, access control, surveillance, and emergency preparedness. The perimeter defences are enhanced, with Category A installations requiring a 10 (ten) foot-high wall topped with anti-scaling devices, regular manned guard posts or electronic surveillance, and comprehensive lighting and CCTV coverage with 90 (ninety) day footage retention. Category B installations, while slightly less stringent, still require an 8 (eight) foot wall with barbed wire or concertina coil and similar surveillance measures. Access control is now more sophisticated, mandating biometric systems at all entry points, integration of door frame and handheld metal detectors, and separate frisking facilities for female staff. The number of gates is minimised, with strict segregation between material and personnel entry points, and all gates are monitored by CCTV. Visitor management is formalised, requiring photo passes, pre-approval for entry into classified zones, and a total ban on unauthorised electronic devices within sensitive areas.

6. **Handling of documents and equipment**: A significantly more comprehensive and prescriptive framework for the handling of documents and equipment compared to the 2014 Manual is introduced in the Manual. It mandates that every ILDC must have a clearly defined data classification policy, treating its absence as a violation. Marking and labelling requirements are more stringent, with explicit instructions for the use of coloured paper, red ink, and clear identification on all physical and electronic media containing classified information.

7. **Subcontracting and consultants**: With the growing involvement of subcontractors and external consultants in defence manufacturing, the Manual imposes strict compliance requirements for all third-party entities. All subcontractors and consultants handling classified information must be bound by a Non-Disclosure Agreement ("**NDA**"), undergo security check and be subject to the Official Secrets Act, 1923. It requires thorough character

and antecedent verification, including police checks, for all personnel involved in sensitive assignments, and stipulates that the terms for retention, handling, and destruction of classified information be explicitly detailed in contracts. The Manual mandates regular internal and external audits, with prompt action and reporting on audit recommendations, ensuring that all parties maintain strict compliance with security protocols to protect national security interests throughout the lifecycle of classified information and materials.

8. **International security**: The Manual mandates the use of GPS tracking for consignments, formalising the requirement for NDA for cross-border transactions involving sensitive or classified information. The Manual specifies that only designated government authorities may authorise and coordinate such transfers. It also requires immediate notification to law enforcement along the transport route and prescribes that classified consignments be shrouded and swiftly removed from public areas upon arrival. These enhancements reflect a shift towards greater procedural rigour, inter-agency coordination, and real-time monitoring, thereby reducing the risk of compromise and ensuring stricter compliance with national security protocols during international transactions.

9. **Audits and compliance**: The Manual mandates a dual-tiered audit system to ensure continuous adherence to security norms:

    a) Internal audit: Both the 2014 Manual and 2025 Manual mandate that internal security audits be conducted at least annually by ILDC, with additional requirements for more frequent checks in multi-facility organisations. These audits are designed to verify adherence to security instructions, assess the effectiveness of existing security and fire control systems, and identify any lapses or vulnerabilities. Following each audit, the auditee must promptly rectify any observations, implement preventive measures, and submit a report of corrective actions to the relevant authorities, such as the Ministry of Home Affairs ("**MHA**") and DDP.

    b) External audits: External audits, carried out by designated government agencies (MHA, MoD, or other nominated bodies), must be carried out at least once every 2 (two) years. The Manual also require annual cyber security audits by the empanelled auditors of the Computer Emergency Response Team - India It stipulates that all audit findings must be addressed in a time-bound manner. Compliance is further reinforced through mandatory self-certification, regular reporting, and the threat of penalties, including licence suspension or cancellation for non-adherence.

10. **Penalties for Non-Compliance**: While similar to the 2014 Manual , the Manual allows for legal action, licence suspension or cancellation (with a 24 (twenty-four) hour requirement to return all classified materials) and reporting of breaches to authorities. The Manual is, however, more explicit and comprehensive: it introduces clear financial penalties, denial of future government contracts, and extends liability to contractors, sub-contractors, and any person involved with the company.

Conclusion

The Manual represents a significant shift in India's security outlook, aligning security protocols with real-time issues. By introducing a dual-category framework, mandating specialised roles like CCSO and CISO, and significantly enhancing both cyber and physical security standards, the Manual addresses legacy issues of the 2014 Manual. The emphasis on audits, international coordination, and third-party accountability reflects a holistic approach to safeguarding national security assets. These reforms will bolster India's credibility as a secure and reliable defence manufacturing hub. The Manual is, thus, both a regulatory upgrade and a strategic enabler for India's Atmanirbhar Bharat ambitions.

Corporate Practice

JSA's corporate practice is centered around transactional and legal advisory services including day-to-day business, regulatory issues, corporate and governance affairs. We have an expert team of attorneys who advise on legal issues concerning inbound and outbound investments, strategic alliances, collaborations and corporate restructurings. We advise clients through all stages of complex and marquee assignments including restructuring, mergers and acquisitions (including those in the public space) to private equity and joint ventures. Our vast clientele includes multinational corporations and large Indian businesses in private, public and joint sector. We work closely with in-house counsel teams, investment banks, consulting and accounting firms along with multilateral agencies and policy making institutions on development of policy and legal frameworks. We provide assistance and counsel to start-ups and venture backed companies by drawing upon our in-depth understanding of how companies are incorporated, financed and grown. With an in-depth understanding of the industry combined with years of expertise, our attorneys provide innovative and constructive solutions to clients in complex transactional engagements. We emphasise teamwork across our wide network of offices across India. This allows us to benefit from the various specialisations available for the ultimate benefit of our clients. We also provide assistance in dealing with diverse corporate governance and compliance issues including FCPA /Anti-Bribery/Anti-Corruption matters and investigations.

This Prism has been prepared by:

Zain Pandit
Partner

Aashna Nahar
Associate

18 Practices and
41 Ranked Lawyers

7 Ranked Practices,
21 Ranked Lawyers

14 Practices and
12 Ranked Lawyers

12 Practices and 50 Ranked Lawyers

20 Practices and
22 Ranked Lawyers

8 Practices and
10 Ranked Lawyers
Highly Recommended in 5 Cities

Recognised in World's 100 best competition practices of 2025

Among Best Overall Law Firms in India and 14 Ranked Practices

---

9 winning Deals in IBLJ Deals of the Year

---

11 A List Lawyers in IBLJ A-List - 2025

Asia M&A Ranking 2024 – Tier 1

Employer of Choice 2024

Energy and Resources Law Firm of the Year 2024

Litigation Law Firm of the Year 2024

Innovative Technologies Law Firm of the Year 2023

Banking & Financial Services Law Firm of the Year 2022

Ranked Among Top 5 Law Firms in India for ESG Practice

2022

Ranked #1
Best Law Firms to Work

Top 10 Best Law Firms for Women

For more details, please contact km@jsalaw.com

jsa
advocates & solicitors

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi