SMLDI 2025 – Nouvelles obligations de sécurité pour l'industrie de défense en Inde

En juin 2025, le Ministry of Defence (MoD) indien a révisé le Security Manual for Licensed Defence Industries (SMLDI), marquant un tournant réglementaire majeur qui redéfinit la manière dont les acteurs privés doivent opérer dans l'écosystème de l'industrie de défense du pays. Publié initialement en 2014, le SMLDI a été entièrement repensé en réponse à l'intensification des menaces géopolitiques, à la multiplication des cyberattaques et à la complexité croissante de la chaîne d'approvisionnement de défense, particulièrement mise en lumière lors de l'Operation Sindoor.

La version révisée du SMLDI s'applique obligatoirement à toutes les entités titulaires d'une licence de fabrication de défense délivrée par le Department for Promotion of Industry and Internal Trade (DPIIT). Elle fixe des exigences strictes en matière de cybersécurité, de protection physique, de surveillance de la chaîne d'approvisionnement, de contrôle du personnel, ainsi que de gestion des données et documents sensibles. L'objectif est clair: protéger les infrastructures de défense de l'Inde en imposant des mesures de sécurité solides et homogènes à l'ensemble des unités industrielles sous licence.

Catégories de produits et obligations au niveau des sites

Le SMLDI distingue :

- **Produits de Catégorie A :** Produits hautement classifiés et sensibles du point de vue de la sécurité, nécessitant le plus haut niveau de protection. Exemples : armes, munitions, explosifs, propulseurs, propulsion, aéronefs, navires de guerre, chars de combat, radars, logiciels, divers types de charges.
- **Produits de Catégorie B :** Produits semi-finis, sous-ensembles ou sous-systèmes d'armes principales, d'équipements, de plateformes, ainsi que certains produits finis moins sensibles, tels que les ensembles d'ailes, les structures assemblées, les canons, les tourelles, l'avionique, etc.

Les entreprises fabriquant à la fois des produits des deux catégories doivent soit séparer physiquement leurs installations, soit appliquer les contrôles de niveau Catégorie A à l'ensemble du site, afin d'éviter toute faille de sécurité.

Gouvernance et leadership en matière de sécurité

Deux postes de direction sont désormais obligatoires :

- **Company Chief Security Officer (CCSO) :** Généralement un ancien officier des forces armées ou de police, chargé de la sécurité physique, de la préparation du site, de la formation du personnel et de la coordination avec les agences gouvernementales.

- **Cyber Information Security Officer (CISO) :** Responsable de l'élaboration et de la mise en œuvre de la stratégie globale de cybersécurité, incluant la planification des audits internes, la détection des menaces et vulnérabilités, la gestion de crise et l'application des politiques, en coordination avec des organismes tels que CERT-IN (Indian Computer Emergency Response Team) et NCIIPC (National Critical Information Infrastructure Protection Centre).

Ces deux postes font l'objet d'une vérification préalable rigoureuse avant nomination, puis d'une réévaluation tous les trois ans afin de préserver l'intégrité du leadership et du contrôle interne.

Renforcement de la cybersécurité

Le SMLDI 2025 donne une place centrale à la défense numérique :

- Des audits annuels de cybersécurité par des auditeurs accrédités CERT-IN sont obligatoires, et leurs conclusions doivent être communiquées directement au MoD.
- L'authentification multifactorielle (MFA), le chiffrement de bout en bout des communications sensibles et le strict respect des directives nationales en matière de cybersécurité sont désormais des exigences de base.
- Les entreprises doivent mettre en place des mécanismes de détection proactive, appliquer des contrôles internes de vulnérabilité et adopter des protocoles clairs de gestion de crise.

Sécurité physique renforcée

Toutes les unités industrielles titulaires d'une licence de défense sont tenues de :

- Ériger des murs d'enceinte de 3 mètres de haut équipés de dispositifs anti-escalade.
- Déployer des systèmes de contrôle d'accès biométriques (ACS) à tous les points d'entrée et de sortie.
- Conserver les enregistrements de vidéosurveillance (CCTV) pendant 90 jours.
- Mettre en place un protocole d'accès à deux niveaux pour les zones à haute sécurité.
- Organiser régulièrement des exercices de réponse d'urgence (intrusion, incendie, attaque armée).

Contrôle et formation du personnel

Tous les employés ayant accès à des zones ou à des documents classifiés ou travaillant dans des zones sensibles doivent se soumettre à une vérification rigoureuse de leurs antécédents, en coordination avec les forces de l'ordre, ainsi qu'à des contrôles périodiques, notamment pour les postes impliquant des données à haut risque. Tout le personnel doit également suivre une formation obligatoire sur la cybersécurité et la sécurité physique. Toute violation, qu'elle soit intentionnelle ou accidentelle, entraîne des mesures disciplinaires et sanctions conformément aux lois en vigueur, notamment l'Official Secrets Act et l'Indian Penal Act.

Traitement des informations classifiées

L'accès aux informations classifiées est désormais réglementé par une structure à cinq niveaux (TOP SECRET, SECRET, CONFIDENTIEL, RÉSERVÉ et NON CLASSIFIÉ). Ces documents doivent être stockés, marqués, transmis et détruits selon des procédures strictes, toutes les interactions étant enregistrées et formellement tracées.

Contrôle des matériaux et de la logistique

Tous les matériaux entrants et sortants (y compris les échantillons et les outils de réparation) doivent être enregistrés dans des registres numériques ou des systèmes ERP/IFS.

Le transport d'articles sensibles ou d'explosifs nécessite une escorte armée, un suivi GPS, une vérification du transporteur et une notification préalable aux autorités locales. La transmission d'informations classifiées nécessite un scellage obligatoire, des enveloppes sécurisées et un agent de supervision désigné.

Sous-traitants et Coordination internationale

Les exigences ne se limitent pas au fabricant principal. Tous les sous-traitants, consultants et partenaires internationaux doivent se conformer aux normes SMLDI. Les visites de ressortissants étrangers dans la région, la zone ou l'usine de fabrication où sont menés des projets liéa au MoD sont soumises à l'accord préalable du MoD. Les collaborations internationales et le transfert d'informations classifiées entre deux pays doivent être régis par des Non-Disclosure Agreements (NDA) exécutoires.

Audits, conformité et contrôle interne

LE SMLDI impose aux entreprises du secteur de la défense les obligations suivantes :

1. Constituer un Security Council au sein de chaque unité industrielle afin de contrôler la conformité interne.
2. Soumettre des rapports trimestriels de conformité au MoD.
3. Réaliser des audits de sécurité internes et externes.
4. Effectuer un audit annuel de cybersécurité par des auditeurs certifiés CERT-In, avec transmission des résultats aux autorités.

Conclusion

Le SMLDI 2025 ne se limite pas à une mise à jour réglementaire : il constitue un cadre stratégique visant à rendre la base industrielle de défense indienne résiliente, sécurisée et prête pour l'avenir. Avec la montée des exigences, les attentes vis-à-vis des acteurs privés, indiens comme internationaux, s'intensifient également. Le respect de ces normes n'est plus facultatif, c'est une condition fondamentale pour participer à la chaîne de valeur de défense nationale. Les entreprises licenciées et leurs partenaires étrangers doivent s'adapter rapidement, mettre en place une gouvernance solide et considérer la sécurité non comme une obligation administrative, mais comme un pilier de l'intégrité souveraine de la défense.

Comment Baker Tilly ASA accompagne les industriels du secteur de la défense

Maîtriser la complexité de la version révisée du SMLDI nécessite bien plus qu'une simple conformité réglementaire: cela requiert un partenaire stratégique. Chez Baker Tilly ASA India, nous proposons une gamme intégrée de services en cybersécurité, gouvernance et gestion des risques, spécifiquement conçus pour répondre aux besoins particuliers du secteur de la défense.

1 – CYBERSÉCURITÉ

Audits de cybersécurité & Gestion de la conformité

En tant qu'auditeurs accrédités CERT-In, nous réalisons des audits cyber complets, incluant l'alignement sur les normes ISO 27001 / 27701 / 42001, les évaluations de conformité aux mandats RBI/SEBI/IRDA, ainsi que les analyses d'écarts conformément aux attentes du CERT-In et du MoD. Nous fournissons des rapports détaillés identifiant les zones de non-conformité, avec des mesures prioritaires et un soutien à la remédiation, y compris la mise à jour des politiques et la mise en œuvre de contrôles, et nous offrons une surveillance continue de la conformité avec des contrôles périodiques.

Risques cyber & Gestion des vulnérabilités

Nos équipes déploient des évaluations de vulnérabilités et tests de pénétration (VAPT), des simulations « red team », des examens de sécurité des applications, ainsi qu'une surveillance du Dark Web, des deep fakes et des réseaux sociaux, afin de détecter de manière proactive les menaces et d'offrir des services de suppression. Nous accompagnons également l'intégration de cadres DevSecOps afin de renforcer la sécurité sur l'ensemble du cycle de développement logiciel.

Analyses forensiques numériques & Réponse aux incidents

Dans l'environnement numérique actuel, les cyberattaques, et en particulier des ransomwares, constituent une menace constante pour les organisations, quelle que soit leur taille. En cas de violation, une réponse rapide et structurée est essentielle. Une équipe dédiée à la réponse aux cyber-incidents intervient alors pour contenir l'attaque et rétablir les opérations.

L'action débute par une évaluation d'impact complète : identification de la cause, du point d'entrée et des mouvements latéraux potentiels. Elle se poursuit par l'éradication des éléments malveillants, le nettoyage des systèmes compromis et la réduction des risques de propagation.

Les obligations réglementaires sont couvertes par un reporting détaillé, et un accompagnement est fourni pour la gestion des sinistres d'assurance cyber. L'investigation forensique et la récupération de données permettent un retour rapide à l'activité, avec un minimum de perturbations.

Au-delà de la remédiation, l'équipe recommande des mesures préventives pour renforcer les dispositifs de cybersécurité et réduire les risques d'incidents futurs L'objectif : non seulement rétablir, mais renforcer la résilience, afin de protéger la continuité d'activité et la réputation de l'organisation.

Intégration sécurisée des technologies

De l'IoT et des déploiements cloud aux dispositifs de contrôle basés sur l'IA, nos experts accompagnent les industriels de la défense dans l'évaluation et l'intégration sécurisée des technologies émergentes, garantissant la résilience tout en respectant les exigences de sécurité nationale.

2 – DUE DILIGENCE EN MATIÈRE D'INTÉGRITÉ & CHAÎNE D'APPROVISIONNEMENT

Vérification du personnel & Prévention des risques internes

Nous effectuons une vérification approfondie des antécédents des employés ayant accès à des zones sensibles ou à des informations classifiées, incluant vérification judiciaire, analyse d'historique de crédit, profilage médiatique et évaluation du comportement éthique.

Risques liés aux tiers & Surveillance de la chaîne d'approvisionnement

Nous accompagnons les entreprises dans l'évaluation et le suivi de leurs sous-traitants, fournisseurs et partenaires logistiques via des vérifications d'intégrité, analyses de conflits d'intérêts, évaluations de réputation et analyses des antécédents juridiques.

Veille commerciale & Due Diligence stratégique

En combinant enquêtes de terrain discrètes et recueil d'informations corroborées, nous identifions les risques cachés liés aux sous-traitants, consultants ou partenaires potentiels de joint-venture, afin de faciliter les décisions préalables à l'engagement.

Traçage d'actifs & Investigations pour fraude

Nos experts forensiques sont spécialisés dans la localisation et l'évaluation d'actifs tangibles et intangibles : biens immobiliers, titres financiers, propriété intellectuelle, biens personnels de grande valeur. Nous apportons notre soutien aux enquêtes sur le détournement d'actifs, les structures de propriété dissimulées et le détournement de fonds, éléments clés pour détecter la fraude interne ou les manquements d'un fournisseur.

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

Lien vers les autres articles