

Third Party Evaluation Study CISF Deployment which are in Sectors Receiving Subsidy (e.g. Fertilizers) and being served by CISF on Cost Reimbursement Basis

Executive Summary

The security of National Fertilizers Limited (NFL) units is of paramount importance, given their role in India's agricultural and industrial ecosystem. The Central Industrial Security Force (CISF) is responsible for protecting these units from security threats, unauthorised access, and potential sabotage. This report evaluates the existing CISF security structure in NFL units, highlighting its operational framework, challenges, and effectiveness. The study aims to provide insights into the security mechanisms, identify gaps, and suggest improvements for enhanced safety and efficiency.

National Fertilizers Limited (NFL) is a crucial public sector enterprise engaged in the production and supply of fertilizers across India. Given the strategic importance of these units, security measures must be robust and well-coordinated. The CISF, a specialised paramilitary force, is responsible for securing various industrial installations, including NFL units. This report explores the CISF security structure within NFL facilities, assessing its effectiveness in mitigating risks and ensuring uninterrupted operations.

The Central Industrial Security Force (CISF) was established in 1969 under the Ministry of Home Affairs to provide security to critical infrastructure, including industrial and public sector establishments. NFL, with multiple production units across India, is a high-priority installation due to the hazardous nature of its products and the potential risks associated with chemical production. The CISF's role in NFL units encompasses perimeter security, surveillance, threat response, and coordination with local law enforcement agencies to prevent security breaches and ensure operational continuity.

Objectives of CISF Security Structure in NFL Units

The primary objectives of the CISF security framework in NFL units include:

1. **Protection of Critical Infrastructure:** Ensuring the security of production plants, storage facilities, and administrative buildings against potential threats.
2. **Surveillance and Threat Detection:** Implementing advanced surveillance systems and patrolling mechanisms to identify and neutralise security risks.
3. **Access Control and Personnel Screening:** Regulating entry and exit points to prevent unauthorised access and ensuring strict verification procedures for employees, contractors, and visitors.
4. **Emergency Response and Crisis Management:** Developing and executing contingency plans to handle security breaches, industrial accidents, and natural disasters effectively.
5. **Coordination with Stakeholders:** Collaborating with NFL management, local law enforcement agencies, and intelligence networks to enhance security preparedness and response.
6. **Training and Preparedness:** Conducting regular security drills, training personnel in crisis management, and upgrading security infrastructure to meet evolving threats.

Methodology

The research methodology adopted in this study is primarily based on qualitative insights, complemented by quantitative research techniques to enhance the depth and reliability of the analysis. (experiences, experiences and challenges) to ensure a comprehensive assessment of CISF security structures in NFL units. The study integrates primary and secondary sources of data, along with a systematic literature review, to provide context and support analysis. The study follows a structured research methodology to assess the CISF security structure in NFL units. The methodology includes the following steps:

1. **Discussion with CISF Security Personnel and NFL Management Staff:** Engaging in detailed discussions with CISF officers and NFL management to understand security protocols, operational challenges, and security concerns at the facility.
2. **Review of Available Literature:** Examining existing reports, policies, and security guidelines to establish a background framework for evaluating security measures in NFL units.
3. **Collection of Primary Data:** Conducting on-site observations, interviews, and surveys to gather first-hand data on security operations, personnel efficiency, and infrastructure adequacy.

4. **Data Analysis and Report Writing:** Analysing collected data to identify security gaps, trends, and areas for improvement, followed by compiling findings into a structured report with recommendations.

Challenges Identified

The evaluation across multiple CISF-deployed NFL units revealed several recurring and unit-specific challenges that impact operational efficiency, security readiness, and risk management:

1. **Manpower Shortages:** Most units reported significant gaps between sanctioned and posted CISF personnel, affecting both the security and fire wings. Critical leadership positions, such as Assistant Commandant (Fire), remain vacant in some units, creating oversight gaps.
2. **Technological Gaps:** Limited CCTV coverage, outdated surveillance infrastructure, absence of drones for aerial monitoring, and insufficient modern security gadgets hinder effective surveillance.
3. **Perimeter and Infrastructure Deficiencies:** Inconsistent boundary wall height, damaged fencing, poorly lit sections, and watchtowers in sub-optimal condition reduce perimeter security effectiveness.
4. **Operational Risks:** Labour-intensive activities, particularly during loading and unloading operations, create opportunities for security breaches. Open walls in bagging plants, nearby settlements, and periodic labour strikes increase vulnerability.
5. **Fire and Hazard Risks:** The presence of highly inflammable and toxic substances such as ammonia, chlorine, and hydrogen pipelines poses significant risks. Inadequate fire-specific leadership in some plants exacerbates the challenge.
6. **Emergency Preparedness Gaps:** Infrequent CISF-led mock drills for plant employees, limited communication tools (e.g., walkie-talkies), poor housekeeping in some areas, and a lack of robust inter-agency coordination impact readiness.
7. **Cyber security Vulnerabilities:** Units with computerised systems often lack regular IT security audits, leaving potential loopholes for cyber threats.
8. **Medical and Welfare Gaps:** Some units lack adequate medical facilities for handling emergencies. CISF accommodation is often temporary or inadequate, impacting personnel welfare and retention.

Recommendations

Based on the overall assessment, the Indian Institute of Public Administration (IIPA) strongly recommends the followings:

- 1. Strengthen Human Resources:** Fill all vacant CISF positions urgently, giving priority to leadership roles like Assistant Commandant (Fire). Ensure sanctioned strength is met across both the security and fire wings to maintain full operational coverage.
- 2. Enhance Perimeter Security:** Expand CCTV surveillance to all critical areas and integrate AI-enabled analytics, motion detection sensors, and thermal imaging to enhance night-time and low-visibility monitoring.
- 3. Improve Mobility for Rapid Response:** Procure additional Quick Reaction Team (QRT) vehicles and a fleet of motorbikes to reduce incident response time and ensure a stronger visible security presence.
- 4. Fire Safety Upgradation:** Modernise firefighting infrastructure by acquiring advanced vehicles, automated suppression systems, and heat-resistant protective gear. Increase the frequency of drills and extend training to contract labour and nearby communities.
- 5. Upgrade Security Gadgets:** Provide CISF with advanced tools such as long-range walkie-talkies, satellite phones, night vision devices, and thermal cameras to handle evolving security threats.

Conclusion

The assessment was carried out through document review, field visits, stakeholder consultations, data verification, and analysis of operational and financial records. The audit covered key functional areas including governance, administration, financial management, monitoring systems, procurement practices, beneficiary outreach, and overall programme impact.