CHAPTER VIII : MINISTRY OF HOME AFFAIRS

Central Reserve Police Force

8.1 IT audit of SELO system of Central Reserve Police Force

Highlights

- Despite incurring an expenditure of Rs. 50.70 crore on the implementation of the SELO system of CRPF, end users are not utilizing most of the applications.
- CRPF does not have an IT policy or IT Steering Committee for implementation of the SELO system.
- Due to lack of requisite application controls in the software, the database had been rendered unreliable and incorrect.
- Inadequate logical access controls exposed the system to the risk of unauthorized access.

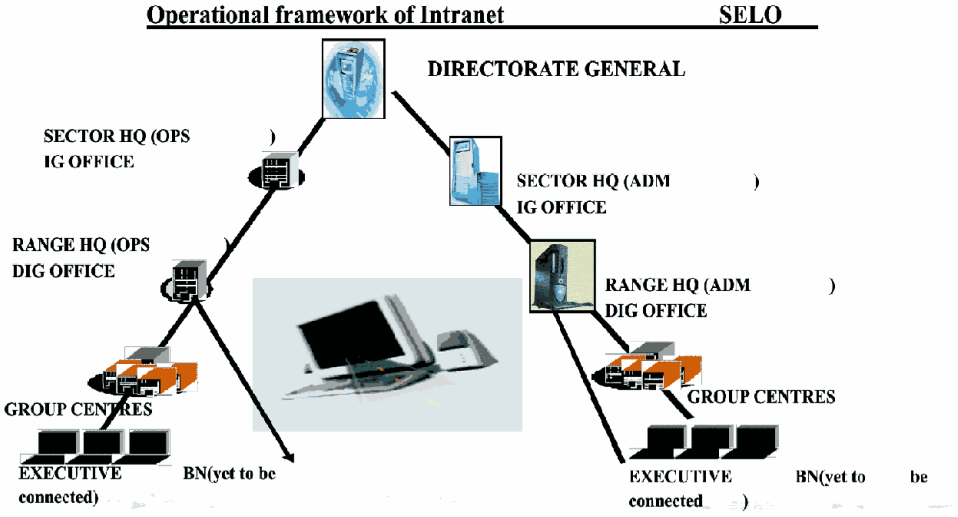
8.1.1 SELO system

Central Reserve Police Force (CRPF) is a Paramilitary force of the Union of India with the basic role of striking reserve to assist the states/union territories in police operations to maintain law and order and contain insurgency. CRPF came into existence as Crown Representative's Police in 1939 and became Central Reserve Police Force on the enactment of CRPF Act in 1949. The Electronic Data Processing (EDP) Cell of CRPF was created in 1972 to computerize the payroll system of Non-Gazetted Officers (NGOs) of 20 battalions. Later in 1985, pay rolls of Gazetted Officers (GOs) and GPF accounts of both GOs and NGOs were also computerized.

In 1997, computerization plan of CRPF was conceived with the aim of introducing information technology in a comprehensive manner. Under the computerization plan, Ministry of Home Affairs (MHA) awarded the development of integrated software named SELO (Service and Loyalty) to M/s NIIT at a cost of Rs. 1.39 crore in March 2000 to be implemented in a phased manner. The first phase of SELO was implemented by networking of 114 CRPF offices from the level of office of the Director General to the Group Centre (GC) offices under Deputy Inspectors General situated at 64 different locations over WAN through leased line connectivity in five stages. MHA[1]

[1] MHA-Ministry of Home Affairs

awarded the implementation work of Stage 1 to IV of SELO at 84 offices situated at 54 different locations, to M/s NIIT in July 2003 at a cost of Rs. 39.07 crore on turn-key basis which was completed in November 2005 with warranty support of 3 years. In stage V, MHA further sanctioned implementation of the SELO project in 30 newly created offices of CRPF at an estimated cost of Rs. 10.24 crore in March 2007. Work at all sites was completed in October 2007 except GC, Bilaspur, which was under progress (July 2009). A detailed plan for the second phase of implementation of SELO in executive battalions was yet to be worked out.



The objective of the SELO CRPF system was to develop an integrated system with latest art of technology. Key features of the system are:

- It covers all functionalities at DG, Sector headquarters, range headquarters, GCs and executive battalions.
- The developed software has web based environment and was menu driven.
- The application contained a Mail and messaging system which act as internal e-mail system in the CRPF.
- A Decision support system (DSS) was also developed as per the requirements of users.

8.1.2 Intended benefits of SELO

- Savings by way of reduction in manpower to the extent of Rs. 8.62 crore *per annum* as envisaged in the proposal of computerization of CRPF.

- Savings due to efficiencies arising in procurement and inventory management envisaged at four *per cent* of the budgetary expenditure and optimal utilization of transport holding

8.1.3 Application modules of the SELO system

The software covers the following modules:

- **Finance**: Budget, finance, audit, TA/DA calculation, LTC, bill preparation, PAO, pension, advances, welfare schemes, funds, library etc.
- **Personnel**: Information relating to recruitments, transfers and deputation of CRPF employees, maintenance of ACRs (Administrative Confidential Records) and Service Books and disciplinary and departmental enquiry cases.
- **Inventory**: Preparation, consolidation and approval of demand and tender, sanction and supply order, receipt/issue and maintenance of stock, condemnation and auction process.
- **Operations**: Masters for various types of code maintenance, movement and deployment and training of personnel, reporting of incidents and intelligence.
- **Payroll:** Monthly salary slips, GPF accounts and income tax calculations.

Each module has mainly four functionalities i.e. master, transaction, reports and decision support system (DSS).

An IT audit of the SELO system revealed the following:

8.1.4 IT Policy

Planning involves the determination of objectives and results, selection of best possible courses of action for achieving the desired result, the time sequence of objectives and the resources required to perform the activities. The absence of a well defined and properly implemented IT policy increases the risk of project failure. Despite incurring an expenditure of Rs. 50.70 crore on computerization, CRPF is yet to formulate and document a formal IT policy and a long term / medium term IT strategy incorporating the time frame, key performance indicators and cost-benefit analysis for effective implementation of the SELO. Further, the lack of a planning/steering committee with clear roles and responsibilities to systematically monitor the implementation of

SELO for each functional area has resulted in non utilisation of the implemented project and also hindered the achievement of objectives for which SELO was implemented. CRPF in its reply (October 2009) stated that a concrete IT policy including all road maps was being prepared.

8.1.5 Achievement of objectives

Phase-I of the SELO system was completed by NIIT across the country at a cost of Rs. 50.70 crore[2] in October 2007. Despite commissioning of the system in October 2007, major activities of CRPF were still carried out manually and end-users were not utilizing the applications available. CRPF, in reply (October 2009) stated that most of the work originates from the battalion levels which were not yet connected to the SELO. Audit, however, observed that CRPF was yet to utilize the SELO in the offices already connected under Phase-I. It was also noticed that the master data in each module were yet to be updated by the EDP cell at DG, CRPF. Due to non utilization of the applications, CRPF is yet to achieve the projected benefits of savings due to manpower reduction and efficient procurement and inventory management. CRPF further stated that steps were being taken to sort out the issues hindering the non usage of the modules.

8.1.6 Post implementation review

Post Implementation Review (PIR) of an existing system is required to ensure that the system met the user requirement specifications and achieved the intended benefits. Despite SELO being in operation for the last four years, post implementation review has not been carried out by CRPF. CRPF in its reply (October 2009) stated that PIR would be undertaken.

8.1.7 Change control mechanism

In order to achieve the desired output, all modifications made to the existing system should be properly authorized, tested, documented and operated as planned. However, audit scrutiny of change request (CR) forms revealed that CR forms for only 319 out of the 786 changes made in the system were available and in 24 out of the 50 CR forms test checked, the name and signature of the person requesting /proposing the changes were not available. Inadequate documentation increases the risk of unauthorized working practices. CRPF in its reply stated that proper documentation would be done as suggested by audit.

---

[2] Stage I to IV(84 offices):Rs. 39.07 crore + Stage V(30 offices): Rs. 10.24 crore +Software: Rs. 1.39 crore = Rs. 50.70 crore

8.1.8 Validation controls

Data analysis of SELO and testing of applications in the training server of CRPF showed that the system lacked proper input and validation checks in different modules. The appointment, nomination and leave records in the personnel module of SELO contained incorrect and unverified data. The personnel data of employees contained multiple duplicate entries for family members and incorrect and blank records for details like name, address, height, weight, basic pay and leave. The details like 'class of city', 'items', 'district', 'police station' and location in the finance, inventory and operations modules which were critical to processing and reporting of financial and operation data were incomplete and incorrect and contained duplicate entries as well. Further, data used for testing purposes were also allowed to remain in the live database. Timely deletion of test data would ensure the reliability of the database. Thus, due to lack of requisite validation and input controls in the software, the database had been rendered unreliable and incorrect. CRPF in its reply (October 2009) stated that validations checks would be incorporated and that after complete verification of personnel data, the data related abnormalities would be eliminated.

8.1.9 IS Security

8.1.9.1 Logical Access controls

Logical access controls protect the programme and data files from unauthorized, modifications, copy and deletions. Though SELO has features of domain controller active directory system to authenticate a user before logging in the system using login ID and password, it had the following deficiencies:

i. The password security policy as per agreement with NIIT was not being implemented, which is vital for the SELO being national integrated application software for all functional areas.

ii. The change of default common password was not mandated by the system after first login and the users continued to access the system using the default passwords.

iii. Normal password control procedures like restriction on unsuccessful login attempts by the users or automatic lapse of passwords after a pre-defined period and periodical change of passwords after certain period were not in existence.

iv. The application system did not have any feature for ensuring password strength in terms of length of password.

CRPF in its reply (October 2009) stated that new password security policy was being formulated for implementation.

8.1.9.2 Segregation of duties

Segregation of duties is essential to ensure transactions are properly authorized, recorded and that assets are safeguarded. The jobs of database administration and system design/support should be separated. It was noticed that the privileges of Database Administrator (DBA) who is the custodian of an organization's data and is responsible for the administration and management of the database systems were also been granted to employees of NIIT helpdesk. Further, the CRPF personnel appointed as DBA is also in charge of support for personnel module. Inadequate segregation of duties increases the risk of error and fraud. CRPF in its reply (October 2009) stated that new policy and guidelines were being formulated for assigning responsibility and access in each module.

8.1.9.3 Firewall and intrusion detection

The major components of security of the datacentre are the firewall and intrusion detection system (IDS). The firewall system secures the network by allowing access to mission control applications on the network to authorized users and keeping unauthorized users out. IDS automatically detects attack patterns from the network traffic, views and monitors intrusion reports on the network. The firewall and IDS of the SELO system were dysfunctional since March 2009 due to lack of support from the manufacturer, exposing the SELO network to unauthorized access. CRPF in its reply (October 2009) stated that proposal was being taken up for adoption of a concrete level of security by enhancing both hardware as well as software based firewall and IDS.

8.1.10 Conclusion

CRPF, one of the prime agencies for the maintenance of internal security of the country developed the SELO system with the objective of computerizing all its functions. It was envisaged that with the implementation of the SELO system savings would be achieved in personnel, inventory and other administrative costs and would help in improving operational efficiency. CRPF had also decided to computerize all areas of its functioning in an integrated manner so that savings would have multiplier effect. However, despite incurring an expenditure of Rs. 50.70 crore on the implementation of the SELO and four years of the launch of the system, most of the activities of

CRPF are still carried out manually. Deficient input controls and validation checks made the available data incomplete, incorrect and unreliable. Inadequate logical access controls, poor segregation of duties combined with dysfunctional firewall and intrusion detection system made the system insecure. Thus, SELO system with unreliable data and security vulnerabilities had the risk of exposing the management of internal security by CRPF to associated threats and shortcomings, even after incurring an expenditure of Rs. 50.70 crore.

Recommendations:

- ❖ CRPF should ensure full utilization of all the SELO applications and move completely from manual to computerized system, as practical, for achieving intended benefits of manpower reduction, efficient procurement utilization and management of inventory and stores.
- ❖ CRPF should have the IT policy and IT steering committee for implementation of the SELO system.
- ❖ CRPF should ensure adequate logical access controls so that security of the data is not compromised. The firewall and intrusion detection system should be made functional to ensure network security.

Adequate validation checks should be embedded in the software systems to avoid erroneous data input and processing.

National Crime Records Bureau

8.2 Non-establishment of Disaster Recovery site for computerised national database of crime records at NIC

NCRB did not establish disaster recovery site to improve the accessibility and security of national database on crime records despite incurring an expenditure of Rs. 54.34 lakh. Meanwhile, the primary objective of maintaining business continuity in the event of break-down of the active site remained unfulfilled.

One of the objectives of the National Crime Records Bureau (NCRB) is to create and maintain secure, sharable, national databases on crimes, criminals, property and also the data pertaining to Motor Vehicles, Firearms and organized crime gangs for law enforcement agencies. The bureau has developed Crime Criminal Information System (CCIS) for collection and dissemination of data which is operational at all the State Crime Records Bureau. The threshold data from all the states is maintained at the NCRB

national server. Government of India in September 2005 declared the data on CCIS as a National Database.

With a view to securing the Database from any disaster, NCRB in January 2006 approached National Informatics Centre (NIC) to co-locate Bureau's data server and application server at the secured data centre of NIC. In response to NCRB's proposal, NIC suggested that NIC data centre would be used as an Active Site for various NCRB applications while NCRB site would be used as a Disaster Recovery (DR) site and furnished an estimate of Rs. 46.75 lakh for procurement of necessary hardware/software. Accordingly NCRB deposited a sum of Rs. 46.75 lakh with NIC in April 2006 for activation of Data centre at NIC and DR site at NCRB. In addition to it, NCRB also purchased equipment worth Rs. 7.59 lakh for operationalisation of the DR site at its own location.

Audit examination disclosed that though NIC had procured necessary hardware and installed it at NIC in April 2007, the Active Site at NIC could not be established, as NIC failed to perceive that the software acquired for replicating data[3] at the data centre was not compatible with the server installed at NIC. Despite advance payment of Rs. 46.75 lakh and protracted correspondence made by NCRB with DG, NIC, the Active Site at NIC and DR Site at NCRB could not be activated/operationalised by NIC as of May 2009. Failure to activate Active/DR Sites even after two years of procurement and installation of hardware highlighted inefficiency of NIC in handling such important projects.

On being pointed out by Audit regarding considerable delay in activation of site, NCRB again approached NIC demi-officially (May 2009) to complete the task on priority but NIC failed to take appropriate action to activate the Site in its premises.

With a view to resolving the site readiness related issues and also the task of Replication Software installation, NCRB in consultation with NIC decided in June 2009 to reverse the earlier decision and decided to create the Active Site at NCRB and the DR Site at NIC and outsource the task to a vendor.

NCRB stated (August 2009) that the active site at NCRB was fully functional but due to non-functioning of the disaster recovery site, backup of data was being kept on tapes. It further added that if the active site went down, users

[3] Replication software replicates the data maintained and updated at a primary site to any alternative site.

from remote locations would not be able to query the database or generate various crime-related reports and efforts were being made to connect the two sites at the earliest. The Ministry also accepted the delay (November 2009) and stated that the action to establish the active site at NCRB and DR site at NIC was being taken by NCRB through an outsourced agency on the advice of NIC and thereafter, needful changes in NCRB network would be taken up on priority as per the advice of NIC. NCRB stated in January 2010 that M/s Wipro had been engaged as Network consultant and LAN configuration settings would be done in consultation with NIC to meet connectivity requirements.

The fact remains that due to lack of appropriate action on the part of NIC, non-setting up the DR site at NIC and storing backup data on tapes exposed NCRB to the risk of not being able to maintain business continuity in the event of breakdown of its active site besides rendering the entire expenditure of Rs. 54.34 lakh idle.