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.