8

STANDING COMMITTEE ON INFORMATION TECHNOLOGY (2004-2005)

FOURTEENTH LOK SABHA

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (DEPARTMENT OF INFORMATION TECHNOLOGY)

[Action taken by Government on the Recommendations/Observations of the Committee contained in their Fifty-Sixth Report (Thirteenth Lok Sabha) on 'Working of National Informatics Centre (NIC)'

EIGHTH REPORT

सत्यमेव जयते

LOK SABHA SECRETARIAT
NEW DELHI

December, 2004/*Agrahayana,* 1926 *(Saka)*

EIGHTH REPORT

STANDING COMMITTEE ON INFORMATION TECHNOLOGY (2004-2005)

(FOURTEENTH LOK SABHA)

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (DEPARTMENT OF INFORMATION TECHNOLOGY)

[Action taken by Government on the Recommendations/Observations of the Committee contained in their Fifty-Sixth Report (Thirteenth Lok Sabha) on 'Working of National Informatics Centre (NIC)'

Presented to Lok Sabha on 14.12.2004
Laid in Rajya Sabha on 14.12.2004

सत्यमेव जयते

LOK SABHA SECRETARIAT
NEW DELHI

December, 2004/*Agrahayana,* 1926 *(Saka)*

CONTENTS

ANNEXURES

COMPOSITION OF THE STANDING COMMITTEE ON INFORMATION TECHNOLOGY (2004-2005)

Shri M.M. Pallam Raju—*Chairman*

MEMBERS

Lok Sabha

2. Shri Nikhil Chaudhary
3. Shri Mani Charenamei
4. Shri Sanjay Dhotre
5. Kunwar Jitin Prasad
6. Shri Kailash Joshi
7. Shri P. Karunakaran
8. Dr. P.P. Koya
9. Shri P.S. Gadhavi*
10. Shri Ajay Maken
11. Smt. Nivedita S. Mane
12. Smt. P. Jayaprada Nahata
13. Col. G. Nizamuddin
14. Shri Sohan Potai
15. Shri Ashok Kumar Rawat
16. Shri Chander Shekhar Sahu
17. Shri Vishnu Sai
18. Shri Tathagat Satpathy
19. Shri K.V. Thangka Balu
20. Shri P.C. Thomas
21. Shri Ram Kripal Yadav

Rajya Sabha

22. Shri Vijay J. Darda
23. Shri Ashwani Kumar
24. Dr. Akhilesh Das

*Nominated *w.e.f.* 20.8.2004.

25. Shri Balbir K. Punj
26. Shri Dara Singh
27. Smt. Sarla Maheshwari
28. Shri N.R. Govindrajar
29. Shri K. Rama Mohana Rao
30. Shri Motiur Rahman
31. Shri Sanjay Nirupam

Secretariat

1. Shri P.D.T. Achary	—	*Additional Secretary*
2. Shri Raj Shekhar Sharma	—	*Deputy Secretary*
3. Shri K.L. Arora	—	*Under Secretary*
4. Shri D.R. Shekhar	—	*Assistant Director*

INTRODUCTION

I, the Chairman of the Standing Committee on Information Technology (2004-05) having been authorised by the Committee to submit the Report on its behalf, present this Eighth Report on Action Taken by Government on the Recommendations/Observations of the Committee contained in their Fifty-Sixth Report (Thirteenth Lok Sabha) on "Working of National Informatics Centre (NIC)" relating to the Department of Information Technology.

2. The Fifty-Sixth Report was presented to Lok Sabha on 22.12.2003 and was laid in Rajya Sabha on 23.12.2003. The Department furnished Action Taken Notes on the recommendations contained in the Report on 3 June, 2004.

3. The Report was considered and adopted by the Committee at its sitting held on 25.11.2004.

4. For facility of reference and convenience, the observations and recommendations of the Committee have been printed in bold letters in the body of the Report.

5. An analysis of Action Taken by Government on the Recommendations/Observations contained in the Fifty-Sixth Report (Thirteenth Lok Sabha) of the Committee is given at Appendix.

NEW DELHI;
7 *December,* 2004
16 *Agrahayana,* 1926 *(Saka)*

M.M. PALLAM RAJU,
Chairman,
Standing Committee on
Information Technology.

CHAPTER I

REPORT

This Report of the Standing Committee on Information Technology deals with the action taken by the Government on the Recommendations/Observations of the Committee contained in its Fifty-Sixth Report (Thirteenth Lok Sabha) on "Working of National Informatics Centre (NIC)" relating to the Department of Information Technology.

2. The Fifty Sixth Report was presented to Lok Sabha on 22.12.2003 and was also laid on the Table of Rajya Sabha on 23.12.2003. It contained 23 Recommendations/Observations.

3. Action Taken Notes in respect of all the Recommendations/Observations contained in the Report have been received and categorised as under :

(i) Recommendations/Observations which have been accepted by the Government:
Paragraph Nos. : 8, 9, 15, 25, 26, 27, 28, 29, 48, 49, 50, 54, 55, 61, 62, 66, 80

Total : 17
Chapter-II

(ii) Recommendations/Observations which the Committee does not desire to pursue in view of the reply of the Government :
Paragraph Nos.: 42, 43, 69, 81

Total : 4
Chapter-III

(iii) Recommendations/Observations in respect of which replies of the Government have not been accepted by the Committee and which require reiteration:
Paragraph Nos. : 77

Total : 1
Chapter-IV

(iv) Recommendations/Observations in respect of which replies are of interim nature:
Paragraph Nos. : 41

Total : 1
Chapter-V

4. The Committee trusts that utmost importance would be given to the implementation of the recommendations accepted by the Government. In cases, for any reason it is not possible for the Ministry to implement the recommendations in letter and spirit, the matter should be reported to the committee with reasons for non-implementation. The Committee further desires that Action Taken Notes on the recommendations/observations contained in Chapter-I of this Report be furnished to it urgently and in no case later than six months of the presentation of the Report.

5. The Committee will now deal with Action Taken by the Government on some of its recommendations.

A. E-GOVERNANCE

(Recommendation Para No. 28)

6. The Committee had desired to know the outcome of e-readiness assessment exercise which was conducted by the Ministry to see up to what extent, the State Governments could provide co-operations for implementing e-governance.

7. The Ministry in their Action Taken Reply have stated as under :

> "The DIT has brought out the India : E-Readiness Assessment Report 2003. It is intended to make this exercise an annual effort. The Report for 2004 is expected to be ready shortly. State Governments have provided the necessary information for compiling the Report."

8. The Committee desires that copies of the report on e-readiness may be made available to them on a continuous basis.

B. NATIONAL INSTITUTE OF SMART GOVERNANCE (NISG)

(Recommendation Para No. 41)

9. The Committee had noted that the National Institute of Smart Governance (NISG)—a joint venture of government, National Association of Software Companies (NASSCOM) and the private sector had been created to play a pivotal role in channelising private resources and competencies into national e-governance efforts and

supplementing the initiatives of National Informatics Centre. The Committee had also noted that out of total shareholding of NISG-entities prescribed holding did not exceed 49% of over all paid up capital of the company. Initial promoters of the company consisted of the Ministry of Information Technology, Ministry of Administrative Reforms, Government of Andhra Pradesh and the NASSCOM. Only nine percent paid up capital was reserved for, other States, which was inadequate and inequitable. The Committee had been given to understand that NISG had been formed at the initiative of Government of Andhra Pradesh and that State had provided ten percent of the equity capital of the Company. The Committee appreciated the initiative of the State Government. However the Committee was at loss to understand why the DoIT did not consult the other State Governments at the stage of the incorporation of the Company and why only nine percent of the equity capital had been earmarked for all of them put together. The Committee had desired that fair share of equity should be reserves for these States and all should be consulted to play a meaningful role for the spread of E-Governance.

10. The Ministry in their reply have stated as under:

> "Various formalities and actions connected with the establishment of the NISG are underway. As soon as these are completed, all States would be invited to participate in the equity of the company.
>
> The DIT is already a stakeholder. The NIC, being an attached office of DIT does not have to be an independent stakeholder.
>
> The NIC and the NISG would be appropriately associated in each other's activities. The NISG is primarily intended to facilitate implementation of Govt. projects involving private sector financial and/or technical resources. Thus there is a complementarity between the roles of the NIC and the NISG."

11. The Committee note that various formalities and actions connected with the establishment of the NISG were underway. On their completion, as per the DIT, all States would be invited to participate in the equity of the company. The Committee would like to be informed about the final outcome of the whole exercise at the earliest.

C. COURT INFORMATION SYSTEM

(Recommendation Para Nos. 48 & 49)

12. The Committee had expressed their happiness over the successful implementation of applications developed for Supreme Court and the High Courts and NIC's proposal to create e-Courts. It would help filing of cases in electronic form, without actually visiting the Supreme Court. The Committee, however, were constrained to note that due to insufficient funds, e-Courts and electronic filing project were yet to be initiated. The Committee were unhappy to note that due to lack of technical manpower, non-replacement of existing Hardware and Software facilities in High Courts, non-availability of good infrastructure at District level, projects at High Courts and District Courts were not taken up by the NIC, thereby delaying the process of timely delivery of justice and access of information to the people.

13. The Committee had, therefore, strongly recommended that sufficient funds be provided on priority basis for serving the legal community through Information Technology. The Committee had further desired to be apprised of the expeditious steps taken by the Government in this regard.

14. The Ministry in their reply have stated as under:

> "The NIC took up the computerization of the Supreme Court and all 18 High Courts (now 21) in 1990 and provided the necessary computer hardware, software and established Local Area Networks. Most of the court officials have been given operational training. The NIC has also worked with the Courts to implement many decision making and decision support systems over the last 13 years. The hardware provided in 1990 has extensively been used and now it requires up-gradation and replacement. Considering the importance of the applications implemented in the Courts, the Government provided an allocation of Rs. 4 crore to the Supreme Court of India. The High Courts of Delhi, Gujarat, A.P. and Karnataka have received funds from the respective State Governments for up-gradation/replacement of obsolete hardware and software.
>
> The NIC has provided the hardware and IT tools in the newly created High Courts of Chhattisgarh, Jharkhand & Uttaranchal

> and implemented several computerized applications. The cost of the project in all the three High Courts was about Rs. 75 lakh.
>
> The Department of Justice, Government of India has, on the basis of the technical proposal submitted by the NIC proposed to upgrade the obsolete hardware and software in the remaining High Courts during 2004-2005. The projected cost of the project is Rs. 35 crore.
>
> The Department of Justice has also taken up the computerization of the City Civil Courts of four Metros, namely: Delhi, Mumbai, Kolkata and Chennai at a cost of Rs. 15 crore. The project in Delhi, Mumbai and Chennai city courts has been implemented. The Kolkata City Civil Courts project is under implementation.
>
> During 2004-2005, the Department of Justice has, on the basis of technical proposals submitted by the NIC, proposed to take up the computerization of all the 31 city Civil Courts at State Capitals. The cost of the project is Rs. 25 crore".

15. The Committee note that the Government have provided an allocation of Rs. 4 crore to the Supreme Court of India for up-gradation and replacement of hardware of 1990 vintage. Also adequate funds have been provided for upgrading the obsolete hardware and software in various High Courts during 2004-2005 by the Department of Justice, Government of India, wherever required. The Department of Justice, Government of India have taken up the computerization of the City Civil Courts of four Metros *viz*. Delhi, Mumbai, Kolkata and Chennai at a cost of Rs. 15 crore and have also proposed to take up the computerization of all the 31 City Civil Courts at State Capitals at a cost of Rs. 25 crore. In this connection, the Committee would like to be apprised of the latest position on different stages of computerization in various courts of the country.

D. LAND RECORDS COMPUTERIZATION PROGRAMME

(Recommendations Paragraph Nos. 61 & 62)

16. The Committee expressed their happiness that the Ministry of Rural development and National Informatics Centre in collaboration, had undertaken computerisation of land records in 586 out of 600

districts in the country. The Committee, however, was perturbed to note that inspite of the fact that the Ministry of Rural development had released assistance of Rs. 264 crore for computerization of land records and installation of hardware and software in 2,782 Tehsil/ Talukas in the country, there had been delay in some States, in completing data entry work due to delay in release of funds by the States to be implementing agencies. The other bottlenecks had been lack of awareness, shortage of manpower and low voltage etc.

17. The Committee had desired that the Ministry should take up the matter with the concerned State Governments at the highest level for timely release of funds to the implementing agencies. The other bottlenecks *viz*., creation of awareness about the scheme, provision of adequate manpower and low voltage should also be taken up with the States so that the scheme which was lagging behind in some States could be completed as early as possible and yield desired benefits to the people.

18. The Ministry in their Action taken reply have stated as under:

> "The NIC role in Land Records Computerization mainly relates to providing computer hardware and software, training and technical support at all districts. Necessary application software with provision of user-friendly data entry, validation, mutation, and backup with in built security mechanism has been designed and developed by NIC as per user requirements in each state. Necessary training on application software is being done regularly by NIC to expedite the implementation. So far NIC has trained more than 6000 revenue officials.
>
> Ministry of Rural Development, which is responsible for this project, has been advised to take-up the matter with the states concerned".

19. The Committee feel that the Ministry of Rural Development which have been provided with such a huge sum of money, should set up an effective monitoring mechanism to oversee the effective utilization of the computer hardware and software to their fullest capacity and towards the intended purpose and objectives. The Committee would like to be continuously apprised of the progress made in the lands record computerization programme.

E. TRAINING OF STAFF

(Recommendation Para No. 77)

20. The Committee were of the considered view that in order to bring about the computer culture in Government offices and assist the user in accepting computer, it was necessary to provide proper and qualitative training to all levels of Government employees. The Committee were given to understand that training/retraining needs of Government officials were so large that the present training resources at various NIC centres, might not be adequate. The Committee, accordingly, keeping in view the importance of training, had desired that Ministry should not only enhance training resources by setting up learning centres at Ministries/Departments with permanent training faculty and computer resources but also increase duration of training courses. The Committee was at loss to understand how much useful training can be imparted in short courses of 2-3 days. The Committee had also desired that Ministry should ensure proper quality of training and its integration with applications in a coordinated manner.

21. The Ministry in their Action Taken Replies have stated as under:

> "All General and Awareness Programmes, Customised Programmes and skill development programmes of NIC are usually for a period of 5 days. However, the short programmes like network basic concepts, Network security, specific product etc. which are of a duration of 2 to 3 days are mostly for those officials who already have basic knowledge and are required to update themselves with latest developments.
>
> The training programmes have been designed and developed by experienced and professional trainers. These programmes have proven to be quite effective.
>
> Technical infrastructure at the NIC State Training Centres is being upgraded in a phased manner beginning from 2003-2004. They are being provided with latest computers and other training tools. For hands-on practice, NIC provides computers to trainees in a 1 : 1 ratio. The project cost is Rs. 4.90 crore.
>
> NIC has also tied up with other agencies for outsourcing specific project based training".

22. The NIC true to its mandate is presently engaged in providing computer communication support to various Central Government Ministries/Departments, High Courts, State Governments, District Headquarters and possibly upto the village panchayat level for various uses. An extension Network NICNET has been spread over 586 Districts linking the Central Government Ministries and Departments with District Administrations, State Secretariats, NCT/UT administrations. In its effort to see that the entire network is utilized, NIC is also providing necessary training which runs in short one time courses of 2-3 days and 5 days. These training programmes cater to specific areas of need thereby exposing the Government staff to a set area of operation/utilization of the computer. Regrettably, the staff is not conversant with the comprehensive use of the computer i.e. for analysis and storing of data etc.

23. Training is a continuous process and updating of the knowledge towards optimum use of the computer requires frequent training. Larger organizations in the private sector are spending upto 5% of the time of an employee on training. A large task force of these organizations is engaged in training so as to keep the staff updated.

24. The Committee feel that considerable time have elapsed since computerization of Government offices was slated and that NIC needs to give a more serious thought to the training aspect so as to be able to get the maximum advantage from the existing infrastructure which has been generated over the years. In order to do so, it has to reconsider its priorities, training content and schedules. The Committee also opine that NIC should concentrate on the higher end needs of the Government in training and it should also play a pivotal role on setting the curriculum of training and decide the training institutes to where most of the training of the Government officials and employees could be outsourced.

CHAPTER II

RECOMMENDATIONS/OBSERVATIONS WHICH HAVE BEEN ACCEPTED BY THE GOVERNMENT

10th Five Year Plan Outlay

Recommendation (Para No. 8)

The Committee finds that the proposed Tenth Plan Outlay of Rs. 705 crore on 'Sustaining on-going activities' of National Informatic Centre has been drastically reduced to Rs. 573 crores. Upgradation/ Expansion schemes have been allocated only Rs. 172 crore against the proposed outlay of Rs. 745 crores. The proposed scheme of E-Infrastructure for e-Governance at Block level which was to cost Rs. 1,500 crore has been completely abandoned. Financial outlay has been thinly spread on Upgradation and Expansion schemes with extension of NICNET getting only Rs. 4,25 crore against the proposal of Rs. 38 crore; e-Governance—Applications and solutions Rs. One crore against the proposal of Rs. 14.50 crores; Development of Multimedia Teleconferencing facility has been allocated Rs. 370 crore against the proposal of Rs. 40 crore recommended by the Department of Information Technology. Again, the ASP Services got only Rs. 2.60 crore, Development Geographic Information System Rs. 2.70 crore and High Speed Terrestrial System Rs. 10 crore against the Departments proposals for Rs. 40 crore, 15 crore and Rs. 100 crore. Thus against an outlay Rs. 3,179.80 crore proposed by the NIC, for Tenth Five Year Plan, Rs. 975 crores have been approved by the Planning Commission. Due to the drastic reduction, various important new schemes envisaged by NIC and ongoing activities including upgradation/extension of NICNET to new districts, e-Governance project, Information Development Programme for North-Eastern States, Info Highway project, computerization projects of Supreme Court, High Court and lower courts etc., will be affected adversely.

Recommendation (Para No. 9)

The Committee is of the opinion that if the National Informatics Centre (NIC) being the premier organization in Government to provide computer based informatics services, for decision support to

Government offices/Bodies at national, State, district and block level, is starved of funds required for execution of its proposed and ongoing schemes, then its basic objectives for which, it has been set up, will be defeated. The Committee is of the considered view that NIC must be provided adequate funds to implement its schemes as envisaged. The Committee, therefore, strongly recommends that Ministry should take up the matter with Planning Commission at the highest level to get the funds released as proposed by the NIC for execution of its ongoing and proposed schemes. The Committee would like to be apprised of the effective steps taken by the Department in this regard.

Action Taken Note

The Department of Information Technology took up the requirement of additional funds at the RE stage. The budget of the NIC was increased from Rs. 181.70 crore to Rs. 201.70 crore in the RE for 2003-2004.

In addition to the above, DIT has released about Rs. 79 crores to the NICSI/NIC during 2003-04 for the implementation of the CIC project (at NE States and J&K State) and for various e-Governance projects.

For the year 2004-05, the Planning Commission has approved an outlay of Rs. 210 crore for the NIC. It has been found adequate for pursuing the various projects of NIC during the current year.

A number of meetings were held with the Planning Commission for provisioning of enhanced budgetary support for the National e-Governance Plan.

The Planning Commission has allocated Rs. 215 crore to DIT for the e-Governance programme for the year 2004-05. One of the major components of this programme is creation of crore infrastructure, including State Wide Area Networks, State Data Centres, National Data Centre and extension/expansion of NICNET.

National Informatics Centre Services Inc. (NICSI)

Recommendation (Para No. 15)

The Committee notes that National Informatics Centre Inc. (NICSI) was set up to promote the economic, scientific, technical, social and cultural development of India by promoting the utilization of Information Technology, Computer Communication network, informatics etc. The Committee recognize the fact that NICSI is setup to supplement the efforts of NIC in providing a mechanism for enhancing the support to NIC for execution of the projects and managing the infrastructure with flexibility which NIC as a conventional government organisation does not have. Also Committee recognizes that NICSI is intimately linked to NIC both in regard to securing of the projects and providing requisite manpower for execution of projects. Therefore, NICSI cannot be considered as any other section 25 company rather it should be seen as an integral wing of NIC who must be authorized to exercise all conceivable control over NICSI seamlessly. The Committee also notes that NICSI which was headed by DG, NIC, is now headed by the Joint Secretary (E-Governance), Department of Information Technology. The Committee is also of the view that for strengthening of NIC and to avoid overlapping of work it is very important that NICSI is fully integrated with NIC as was planned during its creation. NICSI should not only be under the control of NIC but also the Chairman of NICSI be appointed by the NIC as it was before September, 2002.

Action Taken Note

The Articles of Association of NICSI were amended in December 2002 with the concurrence of the Government of India through the NIC, as provided in the Memorandum of Association. As per Article 58 of the revised Articles of Association, the ex-officio directors of the company are:

(1) Shri R. Chandrashekhar, Joint Secretary, Department of Information Technology (DIT)—Chairman.

(2) Dr. Gulshan Rai, Executive Director, ERNET India—Member.

(3) Shri J.K. Tyagi, Deputy Financial Adviser, DIT—Member.

(4) Six Officers from NIC—Members.

Accordingly, in March, 2003, DG, NIC nominated 6 senior officers of the NIC as directors of the Board of NICSI.

Further, as per Article 59 of the revised Articles of Association, the DG, NIC is empowered to appoint and remove the MD, NICSI.

As such, no difficulty is anticipated in integration of NICSI activities with the NIC.

The scope of the National e-Governance Action Plan is very vast and hence requires a quantum increase in the implementation effort. It necessitates the involvement of multiple agencies and harnessing of all competencies available in the country, including those in the public and private sector, to supplement the effort and capacity of the NIC. Some of the activities involving agencies other than the NIC may still require the services of NICSI. Hence, a broader role is envisaged for NICSI extending beyond a supporting function for NIC activities. The reconstitution of the Board of Directors of NICSI has also to be seen in this context.

E-Governance:

Recommendation (Para No. 25)

The Committee fully recognizes the e-Governance in one of the pivotal steps to take India to Information Age. The Committee also recognizes that this is a complex, time consuming, multidisciplinary and multi stakeholder activity. It is therefore very easy to loose track and land up in large investment without commensurating returns. At the same time India has to take calculated initiatives to move forward. The "change management" *i.e.*, from the prevailing practice of physical paper management to management by digital record and from present closed-door information to open information regime, becomes very important issue especially when a nation like India, having large legacy-issues to be handled in migration of Information age. NIC provides the common IT infrastructure, wealth of sustained domain and knowledge through out the country as the basic e-Governance vehicle. The Committee is of the view that various e-Governance initiatives either by Central Government like e-Governance of DIT, other line ministry department of Central Government where the funds from Central Government are provided for should be integrated by NIC into their initiatives so that a common e-Governance infrastructure and common applications can be rolled out for effective sustenance in the long run. Involving State Governments is equally important in this initiative, specially States which are lagging behind, to minimize the fast growing digital gap among different States within the country. This digital gap is leading to gap in almost all sectors like economic, education, health, employment etc.

Recommendation (Para No. 26)

The Committee notes that e-Governance is the use of Information and Communications Technology to improve efficiency, convenience, accessibility and transparency in Government and is expected to become a backbone structure once all Central and State Government Departments are inter-connected for providing unified/single window services and citizen have access to information anytime, anywhere without any hassle. The Committee appreciates the work being done by the Government for achieving the objectives of e-Governance. The State Governments have also been found to be very active in adopting and implementing applications of e-Governance successfully.

Recommendation (Para No. 27)

However, the Committee is constrained to find that many of the States are still lacking in the application of hardware and there is an urgent need to create e-Governance infrastructure by the State Governments for implementation of e-Governance programmes, in most of the States, only some computer applications are being run in specific areas *viz*. Land records, driving licence etc. and not in all areas of e-Governance. The Committee, therefore, agrees with the Ministry that State Governments should atleast earmark 3 per cent of their budget for IT related applications on the lines of Central Government ministries for strengthening of e-Governance and its infrastructure. The Committee, therefore, desires that the views of the Committee may be conveyed to all the concerned State Governments.

Action Taken Note

In this regard, the NIC has already taken up many initiative as noted below:

(a) NICNET has been strengthened up to the level of State Capitals by adding fibre-optic based terrestrial links to the existing satellite connectivity. In addition, connectivity to the district level for various Central Government and State Governments applications has been initiated.

(b) A Data Centre has been established at the NIC Headquarters. A disaster recovery facility has been established at

Hyderabad. Steps are being taken to establish similar facilities at State Headquarters in consultation with State Governments. The objective is to establish a common data storage facility for various applications planned for e-Governance. The first batch of State data centres is at an advanced stage of implementation.

(c) The Planning Commission has effected a substantial increase in the budget of the DIT for 2004-05 for various e-Governance projects, including extension of network connectivity upto block level. Enhanced provisions have also been made in the NIC budget for its activities including strengthening and augmentation of NICNET.

The NIC has been approached by various Central Government Departments to provide network facilities for their applications. Such facilities may be provided by supplementing the existing network (NICNET) with investments by the respective departments, or alternatively by additional provisions in the NIC budget. This is being taken up with the Planning Commission.

Similarly, some State Governments have requested the NIC to establish a network backbone infrastructure, for which States are ready to provide bandwidth, which has been committed to them by the basic telecom service providers in exchange for Right of Way. The NIC is geared up to respond to such requests to establish an extended backbone network for catering to various e-Governance initiatives.

Discussions are being held with State Governments to formalize the policy guidelines for supporting the State Governments in creation of State Wide Area Networks and State Data Centres in an appropriate collaborative mode.

Secretary, DIT has advised Chief Secretaries of all States to allocate at least 3% of the State budget for e-Governance applications and infrastructure in line with the observations of the Standing Committee.

Recommendation (Para No. 28)

The Committee also desires to know the outcome of e-readiness assessment exercise which has been conducted by the Ministry to see up to what extent, the State Governments can provide cooperations for implementing e-Governance.

Action Taken Note

The DIT has brought out the India: E-Readiness Assessment Report 2003. It is intended to make this exercise an annual effort. The Report for 2004 is expected to be ready shortly. State Governments have provided the necessary information for compiling the Report.

Recommendation (Para No. 29)

The Committee notes that a Wide Area Network Infrastructure has been proposed by the State Government of Orissa for computerisation at district, block and Panchayat levels so as to provide benefits of e-Governance applications like Data basic, e-mail, voice-over-IP, work flow automation Video conferencing etc., to its people. The Committee appreciates the dedicated initiatives taken by the State Government of Orissa in building e-Governance infrastructure in the State with a view to have transparent, efficient and employment oriented administrative set up. The Committee desires the Government to consider the requests of the State Government sympathetically and render all possible assistance—financial and technical to the State Governments with a view to expedite implementation of infrastructure and hardware development schemes down below upto Block level. The Committee desires that as early as possible, the State of Orissa be connected with area network for the purpose and sufficient funds as proposed by the State of Orissa to Twelfth Finance Commission be made available so that schemes as envisaged by the State Government can be executed.

Action Taken Note

NIC Orissa unit has been involved in developing & implementing various e-Governance applications at State, District, Block / Tehsil levels as part of its objectives. NICNET has been strengthened in all the 30 districts of Orissa through VSATs, Video facility at 6 locations and RF connectivity at State Secretariat.

The Department of Space had approached NIC (in 2002) to prepare a proposal for connecting all districts and blocks with some of the departments which interact with the districts / blocks for citizen centric applications under the GRAMSAT project. The total estimated cost for this project is Rs. 14.16 crores. On the basis of this proposal, Government of Orissa had released funds to NICSI for implementing the project in association with NIC. This project is under implementation.

Court Information System

Recommendation (Para No. 48)

The Committee is happy to note that NIC has successfully implemented the applications developed for Supreme Court, High Courts and also proposes to create e-Court. It will help filing of cases in electronic form, without actually visiting the Supreme Court. The Committee, however, is constrained to note that due to insufficient funds, e-Courts and electronic filing project are yet to be initiated. The Committee is further unhappy to note that due to lack of technical manpower, non-replacement of existing Hardware and Software facilities in High Courts, non-availability of good infrastructure at District level, projects at High Courts and District Courts are not taken up by the NIC, thereby delaying the process of timely delivery of justice and access of information to the people.

Recommendation (Para No. 49)

The Committee, therefore, strongly recommends that sufficient funds be provided on priority basis for serving the legal community through Information Technology. The Committee would like to be appraised of the expeditious steps taken by the Government in this regard.

Action Taken Note

The NIC took up the computerization of the Supreme Court and all 18 High Courts (now 21) in 1990 and provided the necessary computer hardware, software and established Local Area Networks. Most of the court officials have been given operational training. The NIC has also worked with the Courts to implement many decision making and decision support systems over the last 13 years. The hardware provided in 1990 has extensively been used and now it requires up-gradation and replacement. Considering the importance of the applications implemented in the Courts, the Government provided an allocation of Rs. 4 crore to the Supreme Court of India. The High Courts of Delhi, Gujarat, A.P. and Karnataka have received funds from the respective State Governments for up-gradation/ replacement of obsolete hardware and software.

The NIC has provided the hardware and IT tools in the newly created High Courts of Chhattisgarh, Jharkhand & Uttaranchal and implemented several computerized applications. The cost of the project in all the three High Courts was about Rs. 75 lakh.

The Department of Justice, Government of India has, on the basis of the technical proposal submitted by the NIC proposed to upgrade the obsolete hardware and software in the remaining High Courts during 2004-05. The projected cost of the project is Rs. 35 crore.

The Department of Justice has also taken up the computerization of the City Civil Courts of four Metros, namely: Delhi, Mumbai, Kolkata and Chennai at a cost of Rs. 15 crore. The project in Delhi, Mumbai and Chennai city courts has been implemented. The Kolkata City Civil Courts project is under implementation.

During 2004-05, the Department of Justice has, on the basis of technical proposals submitted by the NIC, proposed to take up the computerization of all the 31 City Civil Courts at State Capitals. The cost of the project is Rs. 25 crore.

Recommendation (Para No. 50)

The Committee understands that the NIC has established a video conferencing facility between a District Court and a jail in Bihar for hearing the case of an under trial without actually bringing him/her to the court premises. The Committee does appreciate the performance of NIC, for establishing a VC facility between a District Court and jail, which helped not only the many under trials but also the judiciary in delivering justice to the desired persons in time. The Committee, therefore desires that video conferencing facilities be developed between District Court and jail, wherever proper police escort and transport facility are not available, in the States/Union Territories at a faster rate so that no under trial prisoner is detained in prison due to non disposal of the case. The Committee also desires that Ministry should make proper study for exploring avenues of possibility, where this video conferencing facility could be extended for reducing the expenditure of public exchequer of the Government. The Committee would like NIC to be asked to examine and submit its report and the

Committee to be apprised about the steps taken by the Ministry in this regard.

Action Taken Note

The Video Conferencing (VC) facility between a Jail and a Court for recording the statements of the under trials has been successfully implemented by the NIC in the State of Bihar. The VC facility obviates the need to bring the undertrials from the jail to the court.

The Department of Justice, Government of India requested the NIC to submit a project proposal for taking up the computerization of four Metros City Civil Courts namely : Delhi, Mumbai, Kolkata and Chennai. This project proposal includes VC facilities. At the time of project implementation, it has been pointed out by the Hon'ble judges of the High Courts, who are the Chairmen of the Project Monitoring Committees, that for effective implementation of the VC facility for the said purpose, the Act concerned needs to be changed for allowing the courts to record the statements of the undertrials and accepting them as recorded in their presence. In case of Delhi City Civil Courts, the matter has been referred to the State Govt. for initiating necessary action. In all the four Metros, the Jail authorities have come forward to implement the VC facilities in their respective State capitals.

Extension of NIC Network

Recommendation (Para No. 54)

The Committee notes that out of 586 Districts covered under NICNET, 21 districts are not provided with NIC NETWORK facility due to lack of infrastructure, site not being ready or NIC staff not being posted. The Committee, keeping in view that NICNET links the Central Government Ministries and Departments with District Administrations, State Secretaries and NCT/UT, Administrations, strongly feels that remaining districts be connected with NICNET expeditiously.

Recommendation (Para No. 55)

The Committee therefore desires that Department of Information Technology should take up the matter with the concerned State Government at the highest level to facilitate the process of availability of the required infrastructure and sites so that required manpower can be provided by the NIC to run the NETWORK at Districts Centre.

Action Taken Note

Out of the 21 new districts reported to the Committee, 11 districts (5 in Jharkhand, 3 in Madhya Pradesh, 1 in Bihar and 2 in Uttaranchal) have been operationalised with required ICT infrastructure.

For the remaining districts, the NIC has requested the District Collectors to allocate adequate space for setting up of NIC District Centres. As soon as the required space is made available, the NIC will release funds for site preparation and also provide Computers and Computer Communication infrastructure. The NIC has also advised the District Collectors to nominate a computer savvy officer of the district collectorate to be trained for supervising the centre until NIC technical manpower is recruited for the district.

Land Records Computerization Programme

Recommendation (Para No. 61)

The Committee is happy to note that the Ministry of Rural Development and National Informatics Centre in collaboration, have undertaken computerization of land records in 586 out of 600 districts in the country. The Committee, however, is perturbed to note that inspite of the fact that the Ministry of Rural Development has released assistance of Rs. 264 crore for computerization of land records and installation of hardware and software in 2,872 Tehsil/Talukas in the country, there has been delay in some States, completing data entry work due to delay in release of funds by the States to the implementing agencies. The other bottlenecks have been lack of awareness, shortage of manpower and low voltage etc.

Recommendation (Para No. 62)

The Committee desires that the Ministry should take up the matter with the concerned State Governments at the highest level for timely release of funds to the implementing agencies. The other bottlenecks *viz.*, creation of awareness about the scheme, provision of adequate manpower and low voltage should also be taken up with the States so that the scheme which is lagging behind in some States could be completed as early as possible and yield desired benefits to the people.

Action Taken Note

The NIC role in Land Records Computerization mainly relates to providing computer hardware and software, training and technical support at all districts. Necessary application software with provision of user-friendly data entry, validation, mutation, and backup with in built security mechanism has been designed and developed by NIC as per user requirements in each State. Necessary training on application software is being done regularly by NIC to expedite the implementation. So far NIC has trained more than 6000 revenue officials.

Ministry of Rural Development, which is responsible for this project, has been advised to take up the matter with the States concerned.

Safety of Secret Files

Recommendation (Para No. 66)

The Committee notes that NIC has adopted all protective mechanism to ensure safety of official websites/files. However, in view of the value of security of these websites/files, the Committee desires that security of the confidential files be reviewed from time to time. The guidelines issued to various Departments be also repeated periodically, so that the same is not lost sight of by them. The Committee also desires that Encryption Policy, which is to be declared, by the Committee set up by Department of Information Technology, be followed strictly by the NIC and users departments to upgrade its security system.

Action Taken Note

The security guidelines issued by the Department of Information Technology will be followed by NIC. Relevant extracts from Information Technology Security guidelines contained in Schedule II to the Rule 19(2) of the IT Act, 2000, are annexed.

DOEACC Centre, Kolkata

Recommendation (Para No. 80)

The Committee is perturbed to note precarious financial health of the erstwhile Regional Computer Centre, Kolkata which has been re-christened as DOEACC Centre. It is pity that DOEACC Centres could not pay their staff salaries regularly. The Committee learnt that erstwhile Centres for Electronics Design and Technology Centres are also running in deficit. The Committee will like to be apprised of the reasons for stoppage of Grant-in-Aid since 1999-2000 and the steps proposed to be undertaken by the Department of Information Technology to restore the financial health of DOEACC Centres. The Committee also desires that besides the adequate funding of RCCs, the infrastructure built there be properly made use of to generate additional resources.

Action Taken Note

After the merger of RCC, Kolkata with DOEACC Society, the following steps have been taken to restore the financial health of the Centre:—

— The scope of activities of the Centre has been extended by including IT Services and Consultancy Projects, apart from IT Education & Training, in their overall activities so that the Centre may get benefits from executing various IT projects of NIC.

— The Centre has been encouraged to introduce new courses in emerging areas. New courses in Bio-informatics have been launched at the Centre which are likely to generate Rs. 30 lakhs per annum. The revenue generation from these courses are likely to increase in the coming years. The Centre is also being facilitated to commence IT Enabled Services-BPO Training Programmes.

— A Project on Training of Trainers in e-Learning is being awarded to the Centre, for which GIA of Rs. 42 lakhs has been allocated to the Centre, of which Rs. 30 lakhs will be released shortly.

— A grant-in-aid of Rs. 50 lakhs has been released to Kolkata Centre during the year 2003-04 and the same amount is likely to be allocated next year.

CHAPTER III

RECOMMENDATIONS/OBSERVATIONS WHICH THE COMMITTEE DO NOT DESIRE TO PURSUE IN VIEW OF THE GOVERNMENT REPLY

National Institute of Smart Government (NISG)

Recommendation (Para No. 42)

The Committee recognize the importance of private investment also in e-Governance initiatives. This issue is very closely linked to the Government policy of out sourcing a service. NIC as the primary agency for e-Governance should have been closely associated with the NISG from the very outset. It is surprising to note that NIC is not even in the; board of directors of NISG. The Committee recommends that for effective coordination of the e-Governance NIC be asked to participate in NISG as a stakeholder. As clarified during the meetings NISG should be restricted to work only in the projects where private participation funding is contemplated, and not to be involved it for projects funded by the Government.

Recommendation (Para No. 43)

The Committee also desires that Ministry should make a study on the possibility of NIC/NISG becoming an effective bridge for private participation, in Government project so that their services can be exploited. Keeping in view the rapid changes in Communications Technology, it has become imperative that NIC/NISG should redefine its role.

Action Taken Note

The DIT is already a stakeholder. The NIC, being an attached office of DIT does not have to be an independent stakeholder.

The NIC and the NISG would be appropriately associated in each other's activities.

The NISG is primarily intended to facilitate implementation of Govt. projects involving private sector financial and/or technical resources. Thus there is a complementarity between the roles of the NIC and the NISG.

Shortage of Staff

Recommendation (Para No. 69)

The Committee is concerned to note that there is a shortage of 183 computer engineers with the NIC and proposal for filling up these vacancies is pending with Ministry of Finance. Because of the same, many of the Engineers' posts at district level are lying vacant. The Committee desires that the Department of Information Technology should expedite the redeployment exercise and then take the matter with the Ministry of Finance to fill up the remaining vacancies, so that overall working of NIC including providing communication computer support to the newly created districts may not suffer. The Committee would like to be apprised about the steps taken by the Ministry in this regard.

Action Taken Note

The request of the NIC for filling up vacant posts and creating additional posts for newly created administrative units was considered in the DIT. It has been decided to adopt a four pronged approach, detailed below:

(i) Vacancies that have arisen within one year may be filled at the entry level.

(ii) In regard to posts which have remained vacant for more than one year, the applicability of the economy instructions of 1993 for automatic abolition of such posts may be examined in respect of a scientific establishment such as NIC. If these instructions apply, the procedure prescribed for revival of posts that have been abolished may be followed.

(iii) Additional posts required for manning new administrative units as per the MoUs entered by NIC with the State Govts. may be created in accordance with the prescribed procedure.

(iv) An exercise is being undertaken to ascertain possibilities of re-deploying existing work-force within the NIC and from amongst its erstwhile units, namely RCC Kolkata and RCC Chandigarh.

Recommendation (Para No. 81)

NIC was created way back in September, 1976 with an allocation of a meagre Rs. 3.44 crores plus a UNDP contribution of US $4.4 million for funding the activities set for it. Over the last about two and a half decades of its existence, NIC has crossed various landmarks towards providing common IT infrastructure, creating vast wealth of sustained domain and IT knowledge, spanned throughout the country and has built-up wherewithal except financial strength, to provide the basic e-governance vehicle. The Committee feels that the requirements and expectations have grown substantially for moving to new Information age. Therefore, NIC as the nodal organization for e-Governance, has to gear up itself to face the challenges. This includes upgrading of NICNET upto each block level and ultimately upto the Village Panchayat levels with a view to provide reliable and safe information backbone, sustain different applications, interface with industry for building their effective participation and lead the e-governance through R & D initiatives. These tasks for NIC to usher in new Information Age will not be easy unless it is given the flexibility and freedom as provided to some of the other organizations in scientific departments like ISRO, BARC, DRDO etc.

Action Taken Note

NIC is expanding the common infrastructure to support the growing e-governance activities and programmes. The demands on NIC for building and supporting various applications have increased manifold. Against this background, it needs skilled manpower to face the various challenges ahead.

Technology has also grown very rapidly. New issues like Cyber security have emerged as concerns and have impacted the service delivery paradigm. Such developments require induction of fresh professionals in NIC with new skills.

Flexibility in a Govt. set up would need to be related to achievement of specific goals/targets (like in the cases of ISRO, BARC etc.). In the case of NIC, almost all its activities address and are closely enmeshed with the needs and activities of various Government departments and organizations at central, state and local government level. This necessarily entails close, continuous engagement with other organizations, as per the latters requirements, rather than the other way around. As such, an autonomous structure may not be suited to the NIC set up having regard to the nature and scope of its activities.

However, flexibility and freedom could be provided within a commercial framework for some of the activities that are akin to normal commercial activities of IT companies that provide various kinds of IT-related services including network services, data centers, technical manpower support, etc.

The role of NIC is being reviewed with reference to the current environment, to enable it to focus on those areas and needs that cannot be met by others, and to work in conjunction with other agencies in areas where there are other options, so that the skills of the premier government in-house IT organization are optimally directed.

CHAPTER IV

RECOMMENDATIONS/OBSERVATIONS IN RESPECT OF WHICH REPLIES OF THE GOVERNMENT HAVE NOT BEEN ACCEPTED BY THE COMMITTEE AND WHICH REQUIRE REITERATION

Training of Staff

Recommendation (Para No. 77)

The Committee is of the considered view that in order to bring about the computer culture in Government offices and assist the user in accepting computer, it is necessary to provide proper and qualitative training to all levels of Government employees. The Committee is given to understand that training/retraining needs of Government official are so large that the present training resources at various NIC centres, may not be adequate. The Committee, accordingly, keeping in view the importance of training, desires that Ministry should not only enhance training resources by setting up learning centres at Ministries/Departments with permanent training faculty and computer resources but also increase duration of training courses. The Committee is at loss to understand how much useful training can be imparted in short courses of 2-3 days. The Committee also desires that Ministry should ensure proper quality of training and its integration with applications in a coordinated manner.

Action Taken Report on Para 77

All General and Awareness Programmes, Customised Programmes and skill development programmes of NIC are usually for a period of 5 days. However, the short programmes like network basic concepts, Network security, specific product etc. which are of a duration of 2 to 3 days are mostly for those officials who already have basic knowledge and are required to update themselves with latest developments.

The training programmes have been designed and developed by experienced and professional trainers. These programmes have proven to be quite effective.

Technical infrastructure at the NIC State Training Centers is being upgraded in a phased manner beginning from 2003-04. They are being provided with latest computers and other training tools. For hands-on practice, NIC provides computers to trainees in a 1 : 1 ratio. The project cost is Rs. 4.90 crore.

NIC has also tied up with other agencies for outsourcing specific project based training.

CHAPTER V

RECOMMENDATIONS/OBSERVATIONS IN RESPECT OF WHICH REPLIES ARE INTERIM IN NATURE

National Institute of Smart Government (NISG)

Recommendation (Para No 41)

The Committee notes that the National Institute of Smart Government (NISG)—a joint venture of Government, National Association of Software Companies (NASSCOM) and the private sector has been created to play a pivotal role in channelising private resources and competencies into national e-governance efforts and supplementing the initiatives of National Informatics Centre. The Committee also notes that out of total shareholding of NISG, entitles prescribed holding does not exceed 49% of over all paid up capital of the company. Initial promoters of the company consists of the Ministry of information Technology, Ministry of Administrative Reforms, Government of Andhra Pradesh and the NASSCOM. Only nine percent paid up capital is reserved for, other States, which is inadequate and inequitable. The Committee understands that NISG has been formed at the initiative of Government of Andhra Pradesh and that State has provided ten percent of the equity capital of the Company. The Committee appreciates the initiative of the State Government. However, the Committee is at loss to understand why the DoIT did not consult the other State Government at the stage of the incorporation of the Company and why only nine percent of the equity capital has been earmarked for all of them put together. The Committee desires that fair share of equity should be reserved for these States and all should be consulted to play a meaningful role for the spread of e-Governance.

Action Taken Note

Various formalities and actions connected with the establishment of the NISG are underway. As soon as these are completed, all states would be invited to participate in the equity of the company.

NEW DELHI;
7 *December*, 2004
16 *Agrahayana*, 1926 *(Saka)*

M.M. PALLAM RAJU,
Chairman,
Standing Committee on
Information Technology.

ANNEXURE I

INFORMATION TECHNOLOGY (IT) SECURITY GUIDELINES

1. Introduction

This document provides guidelines for the implementation and management of Information Technology Security. Due to the inherent dynamism of the security requirements, this document does not provide an exact template for the organizations to follow. However, appropriate suitable samples of security process are provided for guidelines. It is the responsibility of the organizations to develop internal processes that meet the guidelines set forth in this document.

The following words used in the Information Technology Security Guidelines shall be interpreted as follows:

- shall: The guideline defined is a mandatory requirement, and therefore must be complied with.
- should : The guideline defined is a recommended requirement. Non-compliance shall be documented and approved by the management. Where appropriate, compensating controls shall be implemented.
- must: The guideline defined is a mandatory requirement, and therefore must be complied with.
- may : The guideline defined is an optional requirement. The implementation of this guideline is determined by the organisation's requirement.

2. Implementation of an Information Security Programme

Successful implementation of a meaningful Information Security Programme rests with the support of the top management. Until and unless the senior managers of the organization understand and concur with the objectives of the information security programme its ultimate success is in question.

The Information Security Programme should be broken down into specific stages as follows:

(a) Adoption of a security policy;

(b) Security risk analysis;

(c) Development and implementation of an information classification system;

(d) Development and implementation of the security standards manual;

(e) Implementation of the management security self-assessment process;

(f) On-going security programme maintenance and enforcement; and

(g) Training.

The principal task of the security implementation is to define the responsibilities of persons within the organization. The implementation should be based on the general principle that the person who is generating the information is also responsible for its security. However, in order to enable him to carry out his responsibilities in this regard, proper tools, and environment need to be established.

When different pieces of information at one level are integrated to form high value information, the responsibility for its security needs also should go up in the hierarchy to the integrator and should require higher level of authority for its access it should be absolutely clear with respect to each information as to who is its owner, its custodian, and its users. It is the duty of the owner to assign the right classification to the information so that the required level of security can be enforced. The custodian of information is responsible for the proper implementation of security guidelines and making the information available to the users on a need to know basis.

3. Information Classification

Information assets must be classified according to their sensitivity and their importance to the organization. Since it is unrealistic to expect managers and employees to maintain absolute control over all information within the boundariesof the or ganization, it is necessary to advise them on which types of information are considered more sensitive, and how the organization would like the sensitive information handled and protected. Classification, declassification, labeling, storage, access, destruction and reproduction of classified data and the administrative overhead this process will create must be considered. Failure to maintain a balance between the value of the information classified and the administrative burden the classification system places on the organization will result in long-term difficulties in achieiving success.

Confidential is that classification of information of which unauthorised disclosure use could cause serious damage to the organization, *e.g.* strategies planning documents.

Restricted is that classification of information of which unauthorized disclosure/use would not be in the best interest of the organization and/or its customers, *e.g.* design details, computer software (programs, utilities), documentation, organization personnel data, budget information.

Internal use is that classification of information that does not require any degree of protection against disclosure within the company, *e.g.* operating procedures, policies and standards inter office memorandums.

Unclassified is that classification of information that requires no protection against disclosure *e.g.* published annual reports, periodicals.

While the above classifications are appropriate for a general organization view point, the following classifications may be considered:

Top Secret: It shall be applied to information unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for Nation's closest secrets and to be used with great reserve.

Secret: This shall be applied to information unauthorized disclosure of which could be expected to cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information and is the highest classification normally used.

Confidentiality: This shall be applied to information unauthorized disclosure of which could be expected to cause damage to the security of the organisation or could be prejudicial to the interest of the organisation, or could affect the organisation in its functioning. Most information will on proper analysis be classified no higher than confidential.

Restricted: This shall be applied to information which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose.

Unclassified: This is the classification of information that requires no protection against disclosure.

4. Physical and Operational Security

4.1 Site Design

(1) The site shall not be in locations that are prone to natural or man-made disasters, like flood, fire, chemical contamination and explosions.

(2) As per nature of the operations, suitable floor structuring, lighting, power and water damage protection requirements shall be provided.

(3) Construction shall comply with all applicable building and safety regulations as laid down by the relevant Government agencies. Further, the construction must be tamper-evident.

(4) Materials used for the construction of the operational site shall be fire resistant and free of toxic chemicals.

(5) External walls shall be constructed of brick or reinforced concrete of sufficient thickness to resist forcible attack. Ground level windows shall be fortified will study mild steel grills or impact-resistant laminated security glass. All internal walls must be from the floor to the ceiling and must be tamper-evident.

(6) Air-conditioning system, power supply system and uninterrupted power supply unit with proper backup shall be installed depending upon the nature of operation. All ducting holes of the air-conditioning system must be designed so as to prevent intrusion of any kind.

(7) Automatic fire detection, fire suppression systems and equipment in compliance with requirement specified by the Fire Brigade or any other agencies of the Central or State Government shall be installed at the operational site.

(8) Media library, electrical and mechanical control rooms shall be housed in separate isolated areas, with access granted only to specific, named individuals on a need basis.

(9) Any facility that supports mission-critical and sensitive applications must be located and designed for repairability, relocation and reconfiguration. The ability to relocate, reconstitute and reconfigure these applications must be tested as part of the business continuity / disaster recovery plan.

4.2 Fire Protection

(1) Combustible materials shall not be stored within hundred meters of the operational site.

(2) Automatic fire detection, fire suppression systems and audible alarms as prescribed by the Fire Brigade or any other agency of the Central or State Government shall be installed at the operational site.

(3) Fire extinguishers shall be installed at the operational site and their locations clearly marked with appropriate signs.

(4) Periodic testing, inspection and maintenance of the fire equipment and fire suppression systems shall be carried out.

(5) Procedures for the safe evacuation of personnel in an emergency shall be visibly pasted / displayed at prominent places at the operational site. Periodic training and fire drills shall be conducted.

(6) There shall be no eating, drinking or smoking in the operational site. The work areas shall be kept clean at all times.

4.3 Environmental Protection

(1) Water detectors shall be installed under the raised floors throughout the operational site and shall be connected to audible alarms.

(2) The temperature and humidity condition in the operational site shall be monitored and controlled periodically.

(3) Personnel at the operational site shall be trained to monitor and control the various equipments and devices installed at the operational site for the purpose of fire and environment protection.

(4) Periodic inspection, testing and maintenance of the equipment and systems shall be scheduled.

4.4 Physical Access

(1) Responsibilities round the clock, seven days a week, three hundred sixty five days a year for physical security of the systems used for operation and also actual physical layout at the site of operation shall be defined and assigned to named individuals.

(2) Biometric physical access security systems shall be installed to control and audit access to the operational site.

(3) Physical access to the operational site at all times shall be controlled and restricted to authorised personnel only. Personnel authorized for limited physical access shall not be allowed to gain unauthorized access to restricted area within operational site.

(4) Dual control over the inventory and issue of access cards/ keys during normal business hours to the Data Centre shall be in place. An up-to-date list of personnel who possess the cards/keys shall be regularly maintained and archived for a period of three years.

(5) Loss of access cards/keys must be immediately reported to the security supervisor of the operational site who shall take appropriate action to prevent unauthorised access.

(6) All individuals, other than operations staff, shall sign in and sign out of the operational site and shall be accompanied by operations staff.

(7) Emergency exists shall be tested periodically to ensure that the access security systems are operational.

(8) All opening of the Data Centre should be monitored round the clock by surveillance video cameras.

5. Information Management

5.1 System Administration

(1) Each organization shall designate a properly trained “System Administration who will ensure that the protective security measures of the system are functional and who will maintain its security posture. Depending upon the complexity and security needs of a system or application, the system Administrator may have a designated System Security Administrator who will assume security responsibilities and provide physical, logical and procedural safeguards for information.

(2) Organisations shall ensure that only a properly trained System Security Administrator is assigned the system security responsibilities.

(3) The responsibility to create, classify, retrieve, modify, delete or archived information must rest only with the System Administrator.

(4) Any password used for the system administration and operation of trustee services must not be written down (in paper or electronic form) or share with any one. A system for password management should be put in place to cover the eventualities such as forgotten password or changeover to another person in case of System Administrator (or System Security Administrator) leaving the organization. Every instance of usage of administrator’s passwords must be documented.

(5) Periodic review of the access rights of all users must be performed.

(6) The System Administrator must promptly disable access to a user’s account if the user is identified as having left the Data Centre, changed assignments or is no longer requiring system access. Reactivation of the user’s account must be authorized in writing by the System Administrator (Digitally signed e-mail may be acceptable).

(7) The System Administrator must take steps to safeguards classified information as prescribed by its owner.

(8) The System Administrator must authorize privileged access to users only on a need-to-know and need-to-do basis and also only after the authorization is documented.

(9) Criteria for the review of audit trails/access logs, reporting of access violations and procedures to ensure timely management action/response shall be established and documented.

(10) All security violations must be recorded, investigated, and periodic status reports compiled for review by the management.

(11) The System Administrator together with the system support staff, shall conduct a regular analysis of problems reported to and identify any weaknesses in protection of the information.

(12) The System Administrator shall ensure that the data, file and Public Key Infrastructure (PKI) servers are not left unmonitored while these systems are powered on.

(13) The System Administrator should ensure that no generic user is enabled or active on the system.

5.2 Sensitive Information Control

(1) Information assets shall be classified and protected according to their sensitivity and criticality to the organizations.

(2) Procedures in accordance with para 8.3 of these Guidelines must be in place to handle the storage media, which has sensitive and classified information.

(3) All sensitive information stored in any media shall bear or be assigned an appropriate security classification.

(4) All sensitive material shall be stamped or labeled accordingly.

(5) Storage media (*i.e.* floppy diskettes, magnetic tapes, portable hard disks, optical disks, etc.) containing sensitive information shall be secured according to their classification.

(6) Electronic communication systems, such as router, switches, network device and computers, used for transmission of

sensitive information should be equipped or installed with suitable security software and if necessary with an encryptor or encryption software. The appropriate procedure in this regard should be documented.

(7) Procedures shall be in place to ensure the secure disposal of sensitive information assets on all corrupted/damaged or affected media both internal (e.g. hard disk/optical disk) and external (e.g. diskette, disk drive, tapes etc.) to the system. Preferably such affected/corrupted/damaged media both internal and external to the system shall be destroyed.

5.3 Sensitive Information Security

(1) Highly sensitive information assets shall be stored on secure removable media and should be in an encrypted format to avoid compromise by unauthorized persons.

(2) Highly sensitive information shall be classified in accordance with para 3.

(3) Sensitive information and data, which are stored on the fixed disk of a computer shared by more than one person, must be protected by access control software (e.g., password). Security packages must be installed which partition or provide authorization to segregated directories/files.

(4) Removable electronic storage media must be removed from the computer and properly secured at the end of the work session or workday.

(5) Removable electronic storage media containing sensitive information and data must be clearly labeled and secured.

(6) Hard disks containing sensitive information and data must be securely erased prior to giving the computer system to another internal or external department or for maintenance.

5.4 Third Party Access

(1) Access to the computer systems by other organisations shall be subjected to a similar level of security protection and controls as in these Information Technology security guidelines.

(2) In case the Data Centre uses the facilities of external service/ facility (outsourcer) for any of their operations, the use of external service/facility providers (e.g. outsourcer) shall be evaluated in light of the possible security exposures and risks involved and all such agreements shall be approved by the information asset owner. The external service or facility provider shall also sign non-disclosure agreements with the management of the Data Centre/operational site.

(3) The external service/facility provider (e.g. outsourcer) shall provide an equivalent level of security controls as required by these Information Technology Security Guidelines.

5.5 Prevention of Computer Misuse

(1) Prevention, detection and deterrence measures shall be implemented to safeguard the security of computers and computer information from misuse. The measures taken shall be properly documented and reviewed regularly.

(2) Each organization shall provide adequate information to all persons, including management, systems developers and programmes, end-users, and third party users warning them against misuse of computers.

(3) Effective measures to deal expeditiously with breaches of security shall be established within each organisation. Such measures shall include:

(i) Prompt reporting of suspected breach;

(ii) Proper investigation and assessment of the nature of suspected breach;

(iii) Secure evidence and preserve integrity of such material as relates to the discovery of any breach;

(iv) Remedial measures.

(4) All incidents related to breaches shall be reported to the System Administrator or System Security Administrator for appropriate action to prevent future occurrence.

(5) Procedure shall be set-up to establish the nature of any alleged abuse and determine the subsequent action required

to be taken to prevent its future occurrence. Such procedures shall include:

(i) The role of the System Administrator, System Security Administrator and management;

(ii) Procedure for investigation;

(iii) Areas for security review; and

(iv) Subsequent follow-up action.

6. System integrity and security measures

6.1 Use of Security Systems or Facilities

(1) Security controls shall be installed and maintained on each computer system or computer node to prevent unauthorised users from gaining entry to the information system and to prevent unauthorised access to data.

(2) Any system software or resource of the computer system should only be accessible after being authenticated by access control system.

6.2 System Access Control

(1) Access control software and system software security features shall be implemented to protect resources. Management approval is required to authorise issuance of user identification (ID) and resource privileges.

(2) Access to information system resources like memory, storage devices etc. sensitive utilities and data resources and programme files shall be controlled and restricted based on a “need-to-use” basis with proper segregation of duties.

(3) The access control software or operating system of the computer system shall provide features to restrict access to the system and data resources. The use of common passwords such as “administrator” or “president” or “game” etc. to protect access to the system and data resources represent a security exposure and shall be avoided. All passwords used must be resistant to dictionary attacks.

(4) Appropriate approval for the request to access system resources shall be obtained from the System Administrator. Guidelines and procedures government access authorisations shall be developed, documented and implemented.

(5) An Access Control System manual documenting the access granted to different level of users shall be prepared to provide guidance to the System Administrator for grant of access.

(6) Each user shall be assigned a unique user ID. Adequate user education shall be provided to help users in password choice and password protection. Sharing of user IDs shall not be allowed.

(7) Stored passwords shall be encrypted using internationally proven encryption techniques to prevent unauthorised disclosure and modification.

(8) Stored passwords shall be protected by access controls from unauthorised disclosure and modification.

(9) Automatic time-out for terminal inactivity should be implemented.

(10) Audit trail of security-sensitive access and actions taken shall be logged.

(11) All forms of audit trail shall be appropriately protected against unauthorised modification or deletion.

(12) Where a second level access control is implemented through the application system, password controls similar to those implemented for the computer system shall be in place.

(13) Activities of all remote users shall be logged and monitored closely.

(14) The facility to login as another user from one user's login shall be denied. However, the system should prohibit direct login as a trusted user (e.g. root in Unix, administrator in Windows NT or Windows 2000). This means that there must be a user account configured for the trusted administrator. The system requires trusted users to change their effective user name to gain access to root and to re-authenticate themselves before requesting access to privileged functions.

(15) The startup and shutdown procedure of the security software must be automated.

(16) Sensitive Operating System files, which are more prone to hackers must be protected against all known attacks using proven tools and techniques. That is to say no user will be able to modify them except with the permission of System Administrator.

6.3 Password Management

(1) Certain minimum quality standards for password shall be enforced. The quality level shall be increased progressively. The following control features shall be implemented for passwords:

(i) Minimum of eight characters without leading or trailing blanks;

(ii) Shall be different from the existing password and the two previous ones;

(iii) Shall be changed at least once every ninety days; for sensitive system, password shall be changed at least once every thirty days; and

(iv) Shall not be shared, displayed or printed.

(2) Password retries shall be limited to a maximum of three attempted logons after which the user ID shall then be revoked; for sensitive systems. The number of password retries should be limited to a maximum of two.

(3) Passwords which are easy-to-guess (e.g. user name, birth date, month, standard words etc.) should be avoided.

(4) Initial or reset passwords must be changed by the user upon first use.

(5) Passwords shall always be encrypted in storage to prevent unauthorized disclosure;

(6) All passwords used must be resistant to dictionary attacks and all known password cracking algorithms.

6.4 Privileged User's Management

(1) System privileges shall be granted to users only on a need-to-use basis.

(2) Login privileges for highly privileged accounts should be available only from Console and terminals situated with Console room.

(3) An audit trail of activities conducted by highly privileged users shall be maintained for two years and reviewed periodically at least every week by operator who is independent of System Administrator.

(4) Privileged user shall not be allowed to log in to the computer system from remote terminal. The usage of the computer system by the privilege user shall be allowed during a certain time period.

(5) Separate user IDs shall be allowed to the user for performing privileged and normal (non-privileged) activities.

(6) The use of user IDs for emergency use shall be recorded and approved. The passwords shall be reset after use.

6.5 User's Account Management

(1) Procedure for user account management shall be established to cord access to application systems and data. The procedures shall include following:

(i) Users shall be authorised by the computer system owner to access computer services.

(ii) A written statement of access rights shall be given to all users.

(iii) All users shall be required to sign an undertaking to acknowledge that they understand the conditions of access.

(iv) Where access to computer services is administered by service providers, ensure that the service providers do not provide access until the authorization procedures have been completed. This includes the acknowledgment of receipt of the accounts by the users.

(v) A formal record of all registered users of the computer services shall be maintained.

(vi) Access rights of users who have been transferred, or left the organisation shall be removed immediately.

(vii) A periodic check shall be carried out for redundant user accounts and access rights that are not longer required.

(viii) Ensure that redundant user accounts are not re-issued to another user.

(2) User accounts shall be suspended under the following conditions:

(i) when an individual is on extended leave or inactive use of over thirty days. In case of protected computer system, the limit of thirty days may be reduced to fifteen days by the System Administrator.

(ii) immediately upon the termination of the services of an individual.

(iii) suspended or inactive accounts shall be deleted after a two months period. In case of protected computer systems, the limit of two months may be reduced to one month.

6.6 Data and Resource Protection

(1) All information assets shall be assigned an "owner" responsible for the integrity of that data/resource. Custodians shall be assigned and shall be jointly responsible for information assets by providing computer controls to assist owners.

(2) The operating system or security system of the computer system shall:

(i) Define user authority and enforce access control to data within the computer system;

(ii) Be capable of specifying, for each named individual, a list of named data objects (e.g. file, programme) or groups of named objects, and the type of access allowed.

(3) For networked or shared computer systems, system users shall be limited to a profile of data objects required to perform their nadded tastes.

(4) Access controls for any data and/or resources shall be determined as per of the systems analysis and design process.

(5) Application Programmer shall not be allowed to access the productive system.

7. Sensitive System Protection

(1) Secure/tokens/smart cards/bio-metric technologies such as Iris recognition finger .... verification technologies etc. shall be used to complement usage of passwords to access the computer system.

(2) For computer system processing sensitive data, access by other arrangement shall be prohibited or strictly controlled.

(3) For sensitive data, encryption of data in storage shall be considered to protect the confidentiality and integrity.

8. Data Centre Operations Security

8.1 Job Scheduling

(1) Procedures shall be established to ensure that all changes to the job securities are appropriately approved. The authority to approve changes to job schedules shall be clearly assigned.

(2) As far as possible, automated job scheduling should be used. Manual job scheduling should require prior approval from the competent authority.

8.2 System Operations Procedure

(1) Procedures shall be established to ensure that only authorised and correct job system and parameter changes are made.

(2) Procedures shall be established to maintain logs of system activities. Such logs shall be reviewed by a competent

independent party for indication of dubious activities. Appropriate retention periods shall be set for such logs.

(3) Procedures shall be established to ensure that people other than well trained computer operators are prohibited from operating the computer equipment.

(4) Procedures shall be implemented to ensure the secure storage or distribution of all outputs/reports, in accordance with procedures defined by the owner for each system.

8.3 Media Management

(1) Responsibilities for media library management and protection shall be clearly defined and assigned.

(2) All media containing sensitive data shall be stored in a locked room or cabinets, which must be fire resistant and free of topic chemicals.

(3) Access to the media library (both on-site and off-site) shall be restricted to the authorized persons only. A list of personnel authorised to enter the library shall be maintained.

(4) The media containing sensitive and back up data must be stored at three different physical locations in the country, which can be reached in few hours.

(5) A media management system shall be in place to account for all media stored on-site and off-site.

(6) All incoming/outgoing media transfers shall be authorised by management and users.

(7) An independent physical inventory check of all media shall be conducted at least every six months.

(8) All media shall have external volume identification. Internal labels shall be fixed, where available.

(9) Procedures shall be in place to ensure that only authorised addition/removal of media from the library is allowed.

(10) Media retention periods shall be established and approved by management in accordance with legal/regulatory and user requirements.

8.4 Media Movement

(1) Proper records of all movements of computer tapes/disks between on-site and off-site media library must be maintained.

(2) There shall be procedures to ensure the authorized and secure transfer to media to/form external parties and the off-site location. A means to authenticate the receipt shall be in place.

(3) Computer media that are being transported to off-site data backup locations should be stored in locked carrying cases that provide magnetic field protection and protection from impact while loading and unloading and during transportation.

9. Data Backup and Off-site Retention

(1) Back up procedures shall be documented, scheduled and monitored.

(2) Up-to-date backups of all critical items shall be maintained to ensure the continued provision of the minimum essential level of service. These item include:—

(i) Data files;

(ii) Utilities programmes;

(iii) Databases;

(iv) Operating system software;

(v) Applications system software;

(vi) Encryption keys;

(vii) Pre-printed forms; and

(viii) Documentation (including a copy of the business continuity plans).

(3) One set of the original disks for all operating system and application software must be maintained to ensure that a valid, virus-free backup exists and available for use at any time.

(4) Backups of the system, application and data shall be performed on a regular basis. Backups should also be made for application under development are data conversion efforts.

(5) Data backup is required for all systems including personal computers, server and distributed systems and databases.

(6) Critical system data and file server software must have full backups take weekly.

(7) The backups must be kept in an area physically separate from the server. Its critical system data on the LAN represents unique versions of the information assets, then the information backups must be rotated on periodic basis to an off-site storage location.

(8) Critical system data and the file server software must have incremental backup taken daily.

(9) Systems that are completely static may not require periodic backup but should be backed up after changes or updates in the information.

(10) Each LAN/system should have a primary and backup operator to ensure continuity of business operations.

(11) The business recovery plan should be prepared and tested on an annual basis.

10. Audit Trials and Verification

(1) Transactions that meet exception criteria shall be completely and accurately highlighted and reviewed by personnel independent of those that initiate the transaction.

(2) Adequate audit trials shall be captured and certain information needed to determine sensitive events and pattern analysis that would indicate possible fraudulent use of the system (*e.g.* repeated unsuccessful logons, access attempts over a series of days) shall be analyzed. This information includes such information as who, what, when, where, and any special information such as:

(i) Success or failure of the event.

(ii) Use of authentication keys, where applicable.

(3) Automated or manual procedures shall be used to monitor and promptly report all significant security events, such as accesses, which are out-of-pattern relative to time, volume, frequency, type of information asset, and redundancy. Other areas of analysis include:

(i) Significant computer system events (*e.g.* configuration updates, system crashes);

(ii) Security profile changes; and

(iii) Actions taken by computer operations, system administrator, system programmes, and/or security administrators

(4) The real time clock of the computer system shall be set accurately to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.

(5) The real time clock of the computer or communications device shall be set to Indian Standard Time (IST). Further there shall be a procedure that checks and corrects drift in the real time clock.

(6) Computer system access records shall be kept for a minimum of two years, in either hard copy or electronic form. Records, which are of legal nature and necessary for any legal or regulation requirement or investigation of criminal behaviour, shall be retained as per laws of the land.

(7) Computer records of applications transaction and significant events must be retained or a minimum period of two years or longer depending on specific record retention requirements.

11. Measures to Handle Computer Virus

(1) Responsibilities and duties shall be assigned to ensure that all file servers and personal computers are equipped with up-to-date virus protection and detection software.

(2) Virus detection software must be used to check storage drives both internal and external to the system on a periodic basis.

(3) All diskettes and software shall be screened and verified by virus detection software before being loaded onto the computer system. No magnetic media like tape cartridge, floppies etc. brought from outside shall be used on the data file PKI or computer server or personal computer on Intranet and Internet without proper screening and verification by virus detection software.

(4) A team shall be designated to deal with reported or suspected incidents of computer virus. The designated team shall ensure that latest version of anti virus software is loaded on all data, file, PKI servers and personal computers.

(5) Procedures shall be established to limit the spread of viruses to other organization information assets. Such procedures *inter-alia* shall include:

(i) Communication to other business partners and users who may be a risk from an infected resource.

(ii) Eradication and recovery procedures.

(iii) Incident report must be documented and communicated as per established procedures.

(6) An awareness and training programme shall be established to communicate virus protection practices, available controls, areas of high risk to virus infection and responsibilities.

12. Relocation of Hardware and Software

Whenever computers or computer peripherals are relocated (e.g. for maintenance, installation at different sites or storage), the following guidelines shall apply:

(i) All removable media will be removed from the computer system and kept at secure location.

(ii) Internal drivers will be overwritten, reformatted or removed as the situation may be.

(iii) If applicable, ribbons will be removed from printers.

(iv) All paper will be removed from printers.

13. Hardware and Software Maintenance

Whenever, the hardware and software maintenance of the computer or computer network is being carried out, the following should be considered:

(1) Proper placement and installation of Information Technology equipment to reduce the effects of interference due to electromagnetic emanations.

(2) Maintenance of an inventory and configuration chart of hardware.

(3) Identification and use of security features implemented within hardware.

(4) Authorization, documentation and control of change made to the hardware.

(5) Identification of support facilities including power and air conditioning.

(6) Provision of an uninterruptibe power supply.

(7) Maintenance of equipment and services.

(8) Organisation must make proper arrangements for maintenance of computer hardware, software (both system and application) and firmware installed and used by them. It shall be the responsibility of the officer in charge of the operational site to ensure that contract for annual maintenance of hardware is always in place.

(9) Organisation must enter into maintenance agreements, if necessary, with the supplier of computer and communication hardware, software (both system and application) and firmware.

(10) Maintenance personnel will sign non-disclosure agreements.

(11) The identities of all hardware and software vendor maintenance staff should be verified before allowing them to carry out maintenance work.

(12) All maintenance personnel should be escorted within the operational site/computer system and network installation room by the authorized personnel of the organisation.

(13) After maintenance, any exposed security parameters such as passwords, use IDs, and accounts will be changed or reset to eliminate any potential security exposures.

(14) If the computer system, computer network or any of its devices is vulnerable to computer viruses as a result of performing maintenance, system, manager or users shall scan the computer system and its devices and any media affected for viruses as a result of maintenance.

14. Purchase and Licensing of Hardware and Software

(i) Hardware and software products that contain or are to be used to enforce security, and intended for use or interface into any organisation system of network, must be verified to comply with these Information Technology Security Guidelines prior to the signing of any contract, purchase or lease.

(2) Software, which is capable of bypassing or modifying the security system or operating system, integrity features, must be verified to determine that they conform to these Information Technology Security Guidelines. Where such compliance is not possible, then procedures shall be in place to ensure that the implementation and operation of that software does not compromise the security of the system.

(3) There shall be procedures to identify, select, implement and control software (system and application software) acquisition and installation to ensure compliance with the Indian Copyright Act and Information Technology Security Guidelines.

(4) It is prohibited to knowingly instal on any system whether test or production, any software which is not licensed for use on the specific systems or networks.

(5) No software will be installed and used on the system when appropriate licensing agreements do not exist, except during evaluation periods for which the user has documented permission to instal and test the software under evaluation.

(6) Illegally acquired or unauthorized software must not be used on any computer, computer network or data communication equipment. In the event that any illegally acquired or unauthorized software is detected by the System Administrator or Network Administrator, the same must be removed immediately.

15. System Software

(1) All system software options and parameters shall be reviewed and approved by the management.

(2) System software shall be comprehensively tested and its security functionality validated prior to implementation.

(3) All vendor supplied default user IDs shall be deleted or password changed before allowing users to access the computer system.

(4) Versions of system software installed on the computer system and communication devices shall be regularly updated.

(5) All changes proposed in the system software must be appropriately justified and approved by an authorised party.

(6) A log of all changes to system software shall be maintained, completely documented and tested to ensure the desired results.

(7) Procedures to control changes initiated by vendors shall be in accordance with para 21 pertaining to "Change Management".

(8) There shall be no standing "Write" access to the system libraries. All "Write" access shall be logged and reviewed by the System Administrator for dubious activities.

(9) System Programmes shall not be allowed to have access to the application system's data and programme files in the production environment.

(10) Procedures to control the use of sensitive system utilities and system programmes that could bypass intended security controls shall be in place and documented. All usage shall be logged and reviewed by the System Administrator and another person independent of System Administrator for dubious activities.

16. Documentation Security

(1) All documentation pertaining to application software and sensitive system software and changes made therein shall be updated to the current time, accurately and stored securely. An up-to-date inventory list of all documentation shall be maintained to ensure control and accountability.

(2) All documentation and subsequent changes shall be reviewed and approved by an independent authorised party prior to issue.

(3) Access to application software documentation and sensitive system software documentation shall be restricted to authorised personnel on a "need-to-use" basis only.

(4) Adequate backups of all documentation shall be maintained and a copy of all critical documentation and manuals shall be stored off-site.

(5) Documentation shall be classified according to the sensitivity of its contents/implications.

(6) Organisations shall adopt a clean desk policy for papers, diskettes and other documentation in order to reduce the risks of unauthorised access, loss of and damage to information outside normal working hours.

17. Network Communication Security

(1) All sensitive information on the network shall be protected by using appropriate techniques. The critical network devices such as routers, switches and modems, should be protected from physical damage.

(2) The network configuration and inventories shall be documented and maintained.

(3) Prior authorization of the Network Administrator shall be obtained for making any changes to network configuration. The changes made in the network configuration shall be documented. The threat and risk assessment of the network after changes in the network configuration shall be reviewed. The network operation shall be monitored for any security irregularity. A formal procedure should be in place for identifying and resolving security problems.

(4) Physical access to communications and network sites shall be controlled and restricted to authorized individuals only in accordance with para 4.4 pertaining to "Physical Access".

(5) Communication and network systems shall be controlled and restricted to authorize individuals only in accordance with para 6.2—System Access Control.

(6) As far as possible, transmission medium within the Certifying Authority's operational site should be secured against electro magnetic transmission. In this regard, use of Optical Fibre Cable and armoured cable may be preferred as transmission media as the case may be.

(7) Network diagnostic tools, *e.g.*, spectrum analyzer, protocol analyzer should be used on a need basis.

18. Firewalls

(1) Intelligent devices generally known as "Firewalls" shall be used to isolate organisation's data network with the external network. Firewall device should also be used to limit network connectivity for unauthorized use.

(2) Networks that operate at varying security levels should be isolated from each other by appropriate firewalls. The internal network of the organization shall be physically and logically isolated from the Internet and any other external connection by a firewall.

(3) All firewalls shall be subjected to thorough test for vulnerability prior to being put to use and at least half-yearly thereafter.

(4) All web servers for access by Internet users shall be isolated from other data and host servers.

19. Connectivity

(1) Organisation shall establish procedure for allowing connectivity of their computer network or computer system to non-organisation computer system or networks. The permission to connect other networks and computer system shall be approved by the Network Administrator and documented.

(2) All unused connections and network segments should be disconnected from active networks. The computer system/ personal computer or outside terminal accessing an organisation's host system must adhere to the general system security and access control guidelines.

(3) The suitability of new hardware/software particularly the protocol compatibility should be assessed before connecting the same to the organisation's network.

(4) As far as possible, no Internet access should be allowed to database server/file server or server hosting sensitive data.

(5) The level of protection for communication and network resources should be commensurate with the criticality and sensitivity of the data transmitted.

20. Network Administrator

(1) Each organization shall designate a properly trained "Network Administrator" who will be responsible for operation, monitoring security and functioning of the network.

(2) Network Administrator shall regularly undertake the review of network and also take adequate measures to provide physical, logical and procedural safeguards for its security. Appropriate follow-up of any unusual activity or pattern of access on the computer network shall be investigated promptly by the Network Administrator.

(3) System must include a mechanism for alerting the Network Administrator of possible breaches in security, *e.g.*, unauthorized access, virus infection and hacking.

(4) Secure Network Management System should be implemented to monitor functioning of the computer network. Broadcast of network traffic should be minimized.

(5) Only authorized and legal software shall be used on the network.

(6) Shared computer systems, network devices used for business applications shall comply with the requirement established in para 6—System Integrity and Security Measures.

21. Change Management

21.1 Change Control

(1) Procedures for tracking and managing changes in application software, system software, hardware and data in the production system shall be established. Organisational responsibilities for the change management process shall be defined and assigned.

(2) A risk and impact analysis, classification and prioritisation process shall be established.

(3) No changes to a production system shall be implemented until such changes have been formally authorised. Authorisation procedures for change control shall be defined and documented.

(4) Owners/Users shall be notified of all changes made to production system which may affect the processing of information on the said production system.

(5) Fall-back procedures in the event of a failure in the implementation of the change process shall be established and documented.

(6) Procedures to protect, control access and changes to production source code, data, execution statements and relevant system documentation shall be documented and implemented.

(7) Version changes of application software and all system software installed on the computer systems and all communication devices shall be documented. Different versions of application software and system software must be kept in safe custody.

21.2 Testing of Changes to Production System

(1) All changes in computer resource proposed in the production system shall be tested and the test results shall be reviewed and accepted by all concerned parities prior to implementation.

(2) All user acceptance tests in respect of changes in computer resource in production system shall be performed in a controlled environment which includes: (i) Test objectives, (ii) A documented test plan, and (iii) acceptance criteria.

21.3 Review of Changes

(1) Procedures shall be established for an independent review of programme changes before they are moved into a production environment to detect unauthorised or malicious codes.

(2) Procedures shall be established to schedule and review the implementation of the changes in computer resource in the production system so as to ensure proper functioning.

(3) All emergency changes/fixes in computer resource in the production system shall be reviewed and approved.

(4) Periodic management reports on the status of the changes implemented in the computer resource in the production system shall be submitted for management review.

22. Problem Management and Reporting

(1) Procedures for identifying, reporting and resolving problems, such as non-functioning of Certifying Authority's system; breaches in Information Technology security; and hacking, shall be established and communicated to all personnel concerned. It shall include emergency procedures. Periodic reports shall be submitted for management review.

(2) A help desk shall be set up to assist users in the resolution of problems.

(3) A system for recording, tracking and reporting the status of reported problems shall be established to ensure that they are promptly managed and resolved with minimal impact on the user of the computing resources.

23. Emergency Preparedness

(1) Emergency response procedures for all activities connected with computer operation shall be developed and documented. These procedures should be reviewed periodically.

(2) Emergency drills should be help periodically to ensure that the documented emergency procedures are effective.

24. Contingency Recovery Equipment and Services

(1) Commitment shall be obtained in writing from computer equipment and supplies vendors to replace critical equipment and supplies within a specified period of time following a destruction of the computing facility.

(2) The business continuity plan shall be developed which *inter alia* include the procedures for emergency ordering of the equipment and availability of the services.

(3) The need for backup hardware and other peripherals should be evaluated in accordance to business needs.

25. Security Incident Reporting and Response

(1) All security related incidents must be reported to central coordinator, appointed by the management to coordinate and handle security related incidents. This central coordinator shall be the single point of contact at the organization.

(2) All incidents reported, actions taken, follow-up actions, and other related information shall be documented.

(3) Procedures shall be defined for dealing with all security related incidents, including malicious software, break-ins from networks, software bugs which compromised the security of the system.

26. Disaster Recovery/Management

(1) Disaster recovery plan shall be developed, properly documented, tested and maintained to ensure that in the event to a failure of the information system or destruction of the facility, essential level of service will be provided. The disaster recovery framework should include:

(a) emergency procedures, describing the immediate action to be taken in case of a major incident.

(b) fall back procedure describing the actions to be taken to relocate essential activities or support services to a backup site.

(c) restoration procedure, describing the action to be taken to return to normal operation at the original site.

(2) The documentation should include:

(a) definition of disaster;

(b) condition for activating the plan;

(c) stages of crisis;

(d) who will make decisions in the crisis;

(e) role of individuals for each component of the plan;

(f) composition of the recovery team; and

(g) decision making process for return to normal operation.

(3) Specific disaster management plan for critical applications shall be developed, documented, tested and maintained on a regular basis.

(4) Responsibilities and reporting structure shall be clearly defined which will take effect immediately on the declaration of a disaster.

(5) Each component/aspect of the plan should have a person and a backup assigned to its execution.

(6) Periodic training of personnel and users associated with computer system and network should be conducted defining their roles and responsibilities in the event of a disaster.

(7) Test plan shall be developed, documented and maintained. Periodic tests shall be carried out to test the effectiveness of the procedures in the plan. The results of the tests shall be documented for management review.

(8) Disaster recovery plan should be updated regularly to ensure its continuing effectiveness.

ANNEXURE

MINUTES OF THE FOURTEENTH SITTING OF THE STANDING COMMITTEE ON INFORMATION TECHNOLOGY (2004-2005)

The Committee sat on Thursday, 25 November, 2004 from 1100 hours to 1330 hours in Committee Room No. 'G-074, K-Block, Parliament Library Building, New Delhi.

PRESENT

Shri M.M. Pallam Raju — *Chairman*

MEMBERS

Lok Sabha

2. Shri Nikhil Chaudhary
3. Shri Mani Cherenamei
4. Shri Sanjay Dhotre
5. Dr. P.P. Koya
6. Shri P.S. Gadhavi
7. Col. G. Nizamuddin
8. Shri Sohan Potai
9. Shri Chander Shekhar Sahu
10. Shri Ram Kripal Yadav

Rajya Sabha

11. Smt. Sarla Maheshwari
12. Shri N.R. Govindarajar
13. Shri K. Rama Mohana Rao
14. Shri Motiur Rahman

SECRETARIAT

1. Shri Raj Shekhar Sharma	—	*Deputy Secretary*
2. Shri K.L. Arora	—	*Under Secretary*
3. Shri D.R. Shekhar	—	*Assistant Director*

2. At the outset, the Chairman welcomed the Members to the sitting of the Committee. The Committee then took up for consideration the following Draft Reports and adopted the same with certain amendments/modifications:

(i) *** *** ***

(ii) *** *** ***

(iii) *** *** ***

(iv) Draft Report on Action Taken by Government on the Recommendations/Observations of the Committee contained in its Fifty-Sixth Report on "Working of National Informatics Centre (NIC)" relating to Department of Information Technology.

(v) *** *** ***

(vi) *** *** ***

3. *** *** ***

4. The Committee, then, authorised the Chairman to finalise and present the above-mentioned Reports to the House.

The Committee, then, adjourned.

APPENDIX

ANALYSIS OF ACTION TAKEN BY GOVERNMENT ON THE THIRTY-EIGHTH REPORT (THIRTEENTH LOK SABHA)

[*Vide* Paragraph No. 5 of Introduction]

(i) Recommendations/Observations which have been accepted by the Government:

Paragraph Nos. 8, 9, 15, 25-29, 48-50, 54-55, 61-62 & 80

Total 17

Percentage 73.91%

(ii) Recommendations/Observations which the Committee do not desire to pursue in view of the reply of the Government:

Paragraph Nos. 42-43, 69 & 81

Total 4

Percentage 17.39%

(iii) Recommendations/Observations in respect of which replies of the Government have not been accepted by the Committee and which require reiteration:

Paragraph No. 77

Total 1

Percentage 4.35%

(iv) Recommendations/Observations in respect of which replies are of interim nature:

Paragraph No. 41

Total 1

Percentage 4.35%