UNIT 5 GUIDELINES ISSUED BY VARIOUS MINISTRIES

Structure

5.1 Introduction

5.2 Objectives

5.3 Broadband Policy, 2004

5.4 .IN Internet Domain Name – Policy Framework

5.5 Draft Policy Guidelines on Web-site Development, Hosting and Maintenance

5.6 New Telecom Policy 1999 (NTP 1999)

5.7 Information Technology Security Guidelines

5.8 SEBI Guidelines on Internet-based Trading and Services

5.9 Guidelines for Setting up of International Gateways for Internet

5.10 Summary

5.11 Terminal Questions

5.12 Answers and Hints

5.1 INTRODUCTION

Different ministries under the Government of India as also State Governments have come out with guidelines and policy related to information technology. Under the Government of India the most important guidelines pertaining to the information and communication technologies have been issued by the Ministry of Communications and Information Technology and under it the Department of Information Technology and also the Department of Telecommunications. Some other ministries have also issued guidelines for instance relating to e-governance. Guidelines and regulations issued by regulators like the Telecom Regulatory Authority of India also have a strong bearing on the subject. In this unit we would go through some of the more important guidelines and policy statements issued by the ministries, which have a bearing on the universe of cyber laws and regulations in the Indian context.

5.2 OBJECTIVES

After studying this unit you should be able to:

- discuss the guidelines issued by the various ministries of the government of India regarding the various aspects of ICT; and
- analyse how these guidelines have facilitated the growth and accessibility of ICT.

5.3 BROADBAND POLICY, 2004

The Ministry of Communication and Information Technology came out with the Broadband Policy in 2004, recognising the potential of the ubiquitous Broadband service in the growth of GDP and enhancement in quality of life through societal applications including tele-education, tele-medicine, e-governance, entertainment as well as employment generation by way of high speed access to information and web-based communication.

The policy explains: it is a fact that the demand for Broadband is primarily conditioned and driven by Internet and PC penetration. The current level of Internet and Broadband access in the country is low as compared to many Asian countries. Penetration of Broadband, Internet and Personal Computer in the country was 0.02%, 0.4% and 0.8% respectively at the end of December, 2003. Currently, high speed Internet access is available at various speeds from 64 kilobits per second (kbps) onwards and presently an always-on high speed Internet access at 128 kbps is considered as 'Broadband'. While there are no uniform standards for Broadband connectivity, various countries follow various standards. The policy defines Broadband connectivity as:

"An 'always-on' data connection that is able to support interactive services including Internet access and has the capability of the minimum download speed of 256 kilo bits per second (kbps) to an individual subscriber from the Point of Presence (POP) of the service provider intending to provide Broadband service where multiple such individual Broadband connections are aggregated and the subscriber is able to access these interactive services including the Internet through this POP. The interactive services will exclude any services for which a separate licence is specifically required, for example, real-time voice transmission, except to the extent that it is presently permitted under ISP licence with Internet Telephony."

The policy estimates a growth for Broadband and Internet subscribers in the country through various technologies is as follows:

Year Ending	Internet Subscribers	Broadband Subscribers
2005	6 million	3 million
2007	18 million	9 million
2010	40 million	20 million

Therefore in order to give effect to a rapid spread of broadband, the policy proposes a series of measures relating to Optical Fibre Technologies, Digital Subscriber Lines (DSL) on copper loop, Cable TV Network, Satellite Media and several other related issues.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 min.*

Discuss the broad band Policy of the Indian Government.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

5.4 .IN INTERNET DOMAIN NAME – POLICY FRAMEWORK

Department of Information Technology of the Ministry of Communications and Information Technology came up with an .IN Internet Domain Name – Policy Framework and Implementation in October 2004. Globally, there are approximately 60 million Internet domain names registered. Of these, about 40 million are in generic top level domain (gTLD) category, while the remaining 20 million are in country code top level domain (ccTLD) category. The administration of gTLD rests with the Internet Corporation for Assigned Names and Numbers (ICANN), an internationally organized non profit corporation, with membership from different countries and experts in the field. The responsibility for administration of ccTLD, on the other hand, has been entrusted to the individual countries who in general follow the guidelines provided by ICANN. In the gTLD category, .com and .net domains are the most popular, and have registered in largest numbers. In recent times, the ccTLD domain registrations are growing with the countries playing active role in the Internet space.

The policy explains that the system of registration of Internet domain names can facilitate the proliferation of Internet in a country. Many countries have therefore adopted liberal and market friendly policies to register large number of Internet domain names under their country code, broadly consistent with global policy and procedures of domain registration. The policy identified that in India; just under 7000 domains have been registered by the Registry at 2nd

and 3rd levels under .IN country code over the past decade or so. This number does not truly represent the penetration of Information Technology (IT) in India when compared with a number of companies and public institutions engaged in IT and IT enabled services (ITeS). The slow growth of .IN domain has been adjudged to be largely due to the absence of contemporary processes and infrastructure, and an over cautious registration policy followed. It is widely recognised that .IN domain name has untapped growth potential. A proactive policy for .IN domain proliferation can establish the .IN as a globally recognised symbol of India's growth and developments in the area of information technology. Therefore, the policy under the new framework for implementation of .IN Registry focuses on creating liberal, efficient and market friendly processes and a distributed organizational structure.

Under the policy, The National Internet Exchange of India (NIXI), a not-for-profit company formed under section 25 of Indian Companies Act, 1956 promoted by the Department of Information Technology (DIT) in association with the Internet Service Providers Association of India (ISPAI). It has been entrusted with the responsibility of setting up the Registry for .IN country code Top Level Domain name (ccTLD). For this the NIXI will create the .IN Network Information Centre (INNIC) to operate as a Registry for .IN domain in India.

With the implementation of the new policy by INNIC under NIXI, a 100,000 .IN domain name registrations at the end of 1st of its operation year has been targeted, with an average annual growth of 50% over a couple of years thereafter.

The following will be the institutional framework of the .IN Registry:

- The .IN Registry will be a Not-for-Profit organization, and will function as an autonomous body, accountable to the government. Its responsibility will be to maintain .IN domain to ensure its operational stability, reliability and security.
- An executive order through a gazette notification will be issued by the Department of Information Technology (DIT), Government of India according a legal status to the Registry for .IN domain in India. It will also mention the role of National Informatics Centre (NIC), ERNET and the nominated Defense Organization as Registrars for handling .gov.in, edu.in, .ac.in and .mil.in registrations respectively.
- The .IN Registry by itself will not carry out registrations. It will do so through a number of Registrars to be appointed by it through an open process of selection on the basis of transparent eligibility criteria.
- The Registrars will either be ISPs themselves who are connected to the National Internet Exchange of India (NIXI), or use the services of such ISP who is connected to NIXI.

The policy also includes the .In Sunrise Policy and the .IN Domain Name Dispute Resolution Policy (INDRP). Under the sunrise policy, owners of registered Indian trademarks or service marks who wish to protect their marks have been given the opportunity to apply for .IN domain names before the general public.

5.5 DRAFT POLICY GUIDELINES ON WEB-SITE DEVELOPMENT, HOSTING AND MAINTENANCE

The Department of Administrative Reforms and Public Grievances under the Ministry of Personnel, Public Grievances and Pensions issued Draft Policy guidelines on Web-site Development, Hosting and Maintenance for the guidance of other ministries and departments of the government. The guidelines have been laid down with the objective of inspiring and facilitating the "realisation of an e-government, which encompasses interlaid the development and deployment of citizen centric services through web enabled processes, electronic workflows, enabled applications, collaborative partnerships and participation of citizens, clients and stakeholders".

The guidelines recognised that the Web site of a Ministry/Department or its portal which integrates several Websites of its constituent offices and units, is a speedy and effective means for dissemination of information, interaction with people and for delivery of services to citizens. Also that the Portal or Website is significant in terms of its capability and potential in serving as an important link between the government and the citizens. It presents the face of the organization, its mission, vision, functions, activities, performance, etc. It provides features enabling public and stakeholders to give their views/ feedback and in realising digital democracy.

Effective operation and management of the website and associated electronic workflows, re-engineered processes, enhance the quality of governance, help achieve improved productivities and realise envisaged outcomes leading to a responsive and transparent governance leveraging on knowledge, inputs, feedback of citizens and stakeholders.

The guidelines have stated that in order to further the aims and objectives described above, the Website will include the following main contents:-

- Mission, Vision, Objectives, Clients, Charter
- Organizational Set-up and Directory
- Functions
- Constitutional, Legal and Administrative Framework
- Ministry
- Plan, Schemes, Programmes and Projects
- Services offered
- Publications and Reports
- Feedback Mechanism
- Notice Board, what is new?
- Announcements, Press Release, Tenders, Procurement and Disposal
- FAQ and Help
- Archives

5.6 NEW TELECOM POLICY 1999 (NTP 1999)

After the Telecom Policy of 1994, the government came out with a New Telecom Policy in 1999. Some of the provisions have a bearing on cyber-space like the statement on electronic commerce. The policy says, "On-line Electronic Commerce will be encouraged so that information can be passed seamlessly. The requirement to develop adequate bandwidth of the order of 10 Gb on national routes and even terabytes on certain congested important national routes will be immediately addressed to so that growth of IT as well as electronic commerce will not be hampered." Similarly on Internet Telephony the policy says, "Internet telephony shall not be permitted at this stage. However, Government will continue to monitor the technological innovations and their impact on national development and review this issue at an appropriate time". The policy also elaborates on the role of a regulator. The Telecom Regulatory Authority of India (TRAI) was formed in January 1997 with a view to provide an effective regulatory framework and adequate safeguards to ensure fair competition and protection of consumer interests. The Government is committed to a strong and independent regulator with comprehensive powers and clear authority to effectively perform its functions.

Towards this objective the following approach will be adopted:

- Section 13 of The TRAI Act gives adequate powers to TRAI to issue directions to service providers. Further, under section 14 of the Act, the TRAI has full adjudicatory powers to resolve disputes between service providers. To ensure level playing fields, it will be clarified that the TRAI has the powers to issue direction under section 13 to Government (in its role as service provider) and further to adjudicate under section 14 of the Act, all disputes arising between Government (in its role as service provider) and any other service provider.
- TRAI will be assigned the arbitration function for resolution of disputes between Government (in its role as licensor) and any licensee.
- The Government will invariably seek TRAI's recommendations on the number and timing of new licences before taking decision on issue of new licences in future.

The functions of licensor and policy maker would continue to be discharged by Government in its sovereign capacity. In respect of functions where TRAI has been assigned a recommendatory role, it would not be statutorily mandatory for Government to seek TRAI's recommendations.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

Discuss the main feature of the new telecom policy, 1999. How it effected the growth of telecommunication secotr in India?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

5.7 INFORMATION TECHNOLOGY SECURITY GUIDELINES

This document from the Department of Information Technology 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.

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

The Information Security Programme should be broken down into specific stages as follows involving, adoption of a security policy, security risk analysis, development and implementation of an information classification system, development and implementation of the security standards manual, implementation of the management security self-assessment process, on-going security programme maintenance and enforcement and 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 higher 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 are 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.

Information Classification is an important aspect of security and therefore, Information assets must be classified according to their sensitivity and their importance to the organization. Similarly physical and operational security including site design, fire protection, environmental protection and physical access are important.

Information Management tools relating to security would involve system administration, sensitive information control, sensitive information security, third party access, prevention of computer misuse, system integrity and security measures. Security can also be enhanced through the use of security systems or facilities such as system access control, password management, privileged user's management, user's account management, data and resource protection, sensitive systems protection, data backup and off-site retention, audit trails and verification. The guidelines also advises on measures to handle computer virus, relocation of hardware and software, hardware and software maintenance and purchase and licensing of hardware and software.

Installation of Firewalls i.e. intelligent devices used to isolate organization's data network with the external network is also recommended.

5.8 SEBI GUIDENLINES ON INTERNET-BASED TRADING AND SERVICES

The SEBI too through its committee on Internet Based Trading and Services in its meeting held on 2nd August, 2000 has come out with minimum requirements for brokers offering securities trading through wireless medium on wireless application protocol (WAP) platform.

5.9 GUIDELINES FOR SETTING UP OF INTERNATIONAL GATEWAYS FOR INTERNET

The Department of Telecom came out with the guidelines for setting up of international gateways by ISP's. The ISP Policy of Government of India permits the ISPs to set up International Gateway for Internet after obtaining the security clearance, for which the interface of the ISPs shall be with the Telecom Authority. The conditions laid down include

1) Gateways can be established only by the ISP licensees.
2) Gateway has to be within the service area of the ISP.
3) The transmission link between the ISP node/point of presence and the Gateway, if they are not co-located, is regulated as per the ISP license

condition 7.2 i.e. the transmission link should be from DOT, licensed Basic Service Operators, Railways, State Electricity Board, National Power Grid Corporation or any other operator specially authorized to lease such links to ISP.

4) The ISP has to apply to the Telecom Authority for bandwidth (transponder capacity in case of satellite access) giving the detailed requirement. (Both short term and long term).

5) Gateway will be used only for carrying Internet Traffic.

6) All the conditions of the ISP licence would be applicable.

7) The ISP should provide information about all ISPs that would be connected to the gateway. Any change should be intimated immediately to the Telecom Authority.

8) The details of the topology should be provided including the details of how the monitoring equipment will be fitted. Any change in the topology should be informed to the Telecom Authority immediately.

9) International Gateways will not be permitted to be set up in security sensitive areas.

10) The Internet nodes on places of security importance (as identified by security agencies) would be routed through VSNL only. Interconnection of these nodes to other nodes within the country directly is not permitted.

11) The ISP should make available all the billing details of any subscriber on demand by Telecom Authority for upto one year.

12) The ISP should block Internet sites and individual subscribers, as identified by Telecom Authority.

13) The Government (Licensor) reserves the right to make changes in the security considerations.

Individuals/Groups/Organizations are permitted to use encryption upto 40 bit key length in the RSA algorithms or its equivalent in other algorithms without having to obtain permission. However, if encryption equipments higher than this limit are to be deployed, individuals/groups/organizations shall do so with the permission of the Telecom Authority and deposit the decryption key, split into two parts, with the Telecom Authority. The guidelines also advise on measures to handle computer virus, relocation of hardware and software, hardware and software maintenance and purchase and licensing of hardware and software.

5.10 SUMMARY

The guidelines issued by the various ministries also form the integral part of the regulatory environment of the cyberspace. Thus in this unit we have examined some of the important guidelines issued by the various ministries. These include the Broadband Policy, 2004, .IN Internet Domain Name – Policy Framework, Draft Policy Guidelines on Web-site Development, Hosting and

Maintenance, the New Telecom Policy, 1999 (NTP 1999), the Information Technology Security Guidelines, the SEBI Guidelines on Internet-based Trading and Services and Guidelines for Setting up International Gateways for Internet.

5.11 TERMINAL QUESTIONS

1) Discuss the in brief the main features of the guidelines issued by the various ministries of the government of India and their impact on the growth of ICT.
2) Discuss the main feature of the Broadband Policy, 2004.
3) What is the salient feature of the New Telecom Policy of 1999? How has it helped bring about telecom revolution in the country?

5.12 ANSWERS AND HINTS

1) The Ministry of Communication and Information Technology came out with the Broadband Policy in 2004, recognising the potential of the ubiquitous Broadband service in the growth of GDP and enhancement in quality of life through societal applications including tele-education, tele-medicine, e-governance, entertainment as well as employment generation by way of high speed access to information and web-based communication.
2) After the Telecom Policy of 1994, the government came out with a New Telecom Policy in 1999. Some of the provisions have a bearing on cyber-space like the statement on electronic commerce. The policy says, “On-line Electronic Commerce will be encouraged so that information can be passed seamlessly. The requirement to develop adequate bandwidth of the order of 10 Gb on national routes and even terabytes on certain congested important national routes will be immediately addressed to so that growth of IT as well as electronic commerce will not be hampered.” Similarly on Internet Telephony the policy says, “Internet telephony shall not be permitted at this stage. However, Government will continue to monitor the technological innovations and their impact on national development and review this issue at an appropriate time.” The policy also elaborates on the role of a regulator Role of Regulator. “The Telecom Regulatory Authority of India (TRAI) was formed in January 1997 with a view to provide an effective regulatory framework and adequate safeguards to ensure fair competition and protection of consumer interests. The Government is committed to a strong and independent regulator with comprehensive powers and clear authority to effectively perform its functions.