ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

Master of Science (Cyber Security)

Cyber law and Regulation of Cyberspace

(CSP-19)

BLOCK

1 Introduction to Python

UNIT-1
DOMESTIC LAWS: BACKGROUNDER

UNIT-2
INFORMATION TECHNOLOGY ACT – PART I

UNIT-3
INFORMATION TECHNOLOGY ACT – PART II

UNIT-4
INTERNATIONAL TREATIES, CONVENTIONS AND PROTOCOLS CONCERNING CYBERSPACE

UNIT-5
GUIDELINES ISSUED BY VARIOUS MINISTRIES

EXPERT COMMITTEE

Dr. Sarojananda Mishra Professor & Head, Dept. of CSE, IGIT, Sarang	**(Chairman)**
Dr. Manas Ranjan Patra Professor & Head, Dept. of CSE Berhampur University, Bhanja Vihar	**(Member)**
Dr. P K Behera Reader, Dept. of CSE, Utkal University, Vani Vihar, Bhubaneswar	**(Member)**
Sri Malaya Kumar Das Scientist-E, NIC Bhubaneswar, Odisha	**(Member)**
Sh. Pabitrananda Patnaik Scientist-E, NIC, Bhubaneswar, Odiaha	**(Member)**
Dr. Manas Ranjan Senapati Associate Professor, Dept. of Information technology, VSSUT, Burla	**(Member)**
Sh. Girija Prasad Nanda Lead, ETA (Education, Training and Assessment), Infosys, Bhubaneswar	**(Member)**
Sri ChandrakantMallick Consultant (Academic) OSOU, Sambalpur, Odisha	**(Convener)**

M.Sc. in Cyber Security (MSCS)

Course Writer

Mr. Aseem Kumar Patel
Academic Consultant
Odisha State Open University, Sambalpur

Material Production

Dr. Manas Ranjan Pujari
Registrar
Odisha State Open University, Sambalpur

UNIT 1 DOMESTIC LAWS: BACKGROUNDER

Structure

1.1 INTRODUCTION

This is the first unit of the first block of Course 2. This unit discusses the main challenges posed by information and communication technology to the law. This unit also gives an overview of the IT Act, 2000 and discusses the amendments suggested by the expert committee set up by the government.

The phenomenal growth of Information and Communication Technology has in a span of a few years significantly changed our way of life. It has changed the way of business, governance, communication, education, entertainment almost every conceivable activity in society. Computers and internet connectivity along with the phenomenal advance in telephony have been the foundation of this revolution.

We are now in the age of the information society wherein it is recognised that "information and communication are at the core of human progress. Rapid progress of these technologies opens completely new opportunities to attain higher levels of development."(From the Declaration of Principles, World Summit on the Information society, 'Geneva 2003 and Tunis 2005). It has been realised that this technology can in benefit millions of people and therefore governments as well as other stake holders have a key role in promoting the spread of the use of the technology more so with the intent to bridge the digital divide that represents the uneven distribution of the benefits of information technology today.

India today is emerging as a global information technology powerhouse, offering high quality IT and IT enabled services at low cost and therefore the IT sector is of immense importance and of great priority for the government. The sector is witnessing rapid growth with exports to the tune of Rs. 78,230 crores in 2004-5. This growth also has a significant effect on the Indian economy. This sector has also risen to become the biggest employment generator in the

country, the number rising from 2.8 lakhs in 1999-2000 to 10 lakhs in 2004-05. Apart from the direct impact on national income and employment, the IT sector has contributed to the growth of several ancillary businesses such as transportation, catering etc. The country has also witnessed a real estate boom stemming from the boom in the IT sector.

The phenomenal connectivity of the net has logically led it to become the most potential instrument for economic activity and governance; **e-commerce** and **e-governance**. With the development of this new technology, and with the realisation that such technology affects human life and relations, societal peace and order and proprietary rights, it was felt that there was a need for laws to regulate conduct in cyberspace accordingly. The need to regulate was also felt because of the immense potential that the medium has to contribute towards development, which can be achieved only through an optimum policy and legal regime governing it. Thus the Internet which as a medium has had a *laissez faire* growth with 'netizens' all over the globe voluntarily contributing substantially to its expansion is now coming more and more within the ambit of governmental regulation. Regulations relating to the Internet are being made today by national government and also by international intergovernmental bodies and international organizations. The whole body of laws and regulations both national and international governing cyberspace constitutes what is known as cyber laws. This however does not mean that the cyberspace does not continue to be an area of expression and innovation for adventurers. Almost on a daily basis human innovation and expression is visible on the Internet.

While going through this and subsequent 2 units, it is recommended that you should keep a copy of the IT Act with you because on many occasions you would find it beneficial to read the sections and subsections of the Act relevant to the topic you are studying.

1.2 OBJECTIVES

After studying this unit you should be able to:

- discuss the challenges which the law should address to keep pace with the new information and communication technology;
- describe the legislative measures taken by India to address the challenges;
- examine as to what extent the IT Act has been able to address the challenges posed by the information and communication technology; and
- discuss the amendments as suggested by experts to make the more effective Act in regulating the area.

1.3 CHALLENGES TO LAWS

The biggest challenge to the law is to keep pace with technology. While talking about crimes relating to the Internet, most traditional crimes like fraud, defamation committed while using the Internet etc, would be governed by the existing technology neutral criminal laws. These are crimes with all elements of offline crimes, the only difference being that the Internet was used as an aid in their commission.

The second kind of crime is the one directed at computers, networks, data etc. These are the crimes that need to be newly defined and prohibited for the purpose of maintenance of order. They include unauthorized disruption of computers and networks, the heart of what most people consider cyber crime. It occurs when an entity, without permission, interferes with the functionality of computer software or hardware. They are more familiar as viruses, worms, logic bombs, Trojan horses, and denial-of-service attacks. Unauthorized access to computer programs and files and theft of identity are the other categories of offences directed at computers.

Some of the challenges of making technology based laws are that there is a chance of them being soon outdated. Therefore, it is desirable that laws as far as possible must be drafted in a technology neutral way. Again it is against equity and fairness if offline conduct is governed differently from online conduct. This give rise to the possibility of crime shifting from one place to the other if there is an inconsistency in laws. Consistency between the two laws is therefore desirable. Laws must also cater to the need of prevention and investigation of crimes. For instance, with the advent of telephones, wire tapping laws were introduced, similar laws to deal with unlawful conduct in the Internet would become necessary.

The first technology based law in India was the Indian Telegraph Act of 1885. This law was framed with the advent of the telegraph and later covered yet another advance in technology, the telephone. In the domain of technology driven law falls the Information Technology Act, 2000.While the Information Technology Act is the most significant Act addressing conduct in cyberspace in India, there are a whole lot of other Acts that would apply to govern and regulate conduct and transactions in cyberspace. Take for instance online contracts. Apart from the relevant provisions of the IT Act like Sections 12 and 13, the Indian Contract Act, the Sale of Goods Act, 1930 etc would be relevant to determine the legality of such contracts. Further the provisions of the Competition Act, 2002 or in case of unfair trade practices, the Consumer Protection Act 1986, would also be relevant.

Protection of intellectual property available on the Internet is one of the greatest challenges of the day. Be it books, films, music, computer software, inventions, formulas, recipes, everything is available on the net. Protection of copyrights trademarks online would entail the invocation of the Indian Copyright Act and, the Trade Marks Act.

As far as illegal activities on the net are concerned, apart from specific provisions in the IT Act that penalizes them, a whole gamut of other Acts would govern them. For instance in case of an Internet fraud, based on the nature of the fraud perpetrated, Acts such as the Companies Act, 1956, the Securities and Exchange Board of India Act, the Banking Regulation Act, the Public Gambling Act, 1867 and the Indian Penal Code would also apply. For online pornography while section 67 of the IT Act would apply, section 293-294 of the IPC as well as the Cinematograph Act, 1952, the Indecent Representation of women Act and the Young Persons (Harmful Publications) Act, 1956 would apply. For matters relating to Internet sale of prohibited

substances like arms and narcotics the Arms Act, 1959, the Explosives Act, 1884, the Narcotic Drugs and Psychotropic substances Act, 1985 would apply.

Thus it can be inferred that while the IT Act is the quintessential Act regulating conduct on the Internet based on the facts of a case or the nature of a transaction, several other Acts may be applicable. Therefore, cyber laws includes the whole set of legislation that can be applied to determine conduct on the Internet.

The march of technology demands the enactment of newer legislation both to regulate the technology and also to facilitate its growth. The next to be soon seen in the statute book is the Act on Communication Convergence, which since 2001 is a Bill. This Act proposes to facilitate development of a national infrastructure for an information based society, and to enable access thereto; to provide a choice of services to the people with a view to promoting plurality of news, views and information; to establish a regulatory framework for carriage and content of communications in the scenario of convergence of telecommunications, broadcasting, data-communication, multimedia and other related technologies and services; and to provide for the powers, procedures and functions of a single regulatory and licensing authority and of the Appellate Tribunal. The communications commission is the key institution in the Bill that is responsible for all matters relating to regulation of communications. Among its main functions are to ensure:

i) that the communication sector is developed in a competitive environment and in consumer interest;

ii) that communication services are made available at affordable cost to all, especially uncovered areas including the rural, remote, hilly and tribal areas;

iii) that there is increasing access to information for greater empowerment of citizens and towards economic development;

iv) that quality, plurality, diversity and choice of services are promoted;

v) that a modern and effective communication infrastructure is established taking into account the convergence of information technology, media, telecommunication and consumer electronics;

vi) that defense and security interests of the country are fully protected;

vii) that introduction of new technologies, investment in services and infrastructure and maximization of communication facilities and services (including telephone density) are encouraged;

viii) that equitable, non-discriminatory interconnection across various networks is promoted;

ix) that licensing and registration criteria are transparent and made known to the public;

x) that an open licensing policy allowing any number of new entrants is in place; and

xi) that the principle of a level playing field for all operators, including existing operators on the date of commencement of this Act, is promoted, so as to serve consumer interest.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

Discuss the reason which necessitate the regulation of cyberspace.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

1.4 INFORMATION TECHNOLOGY ACT, 2000

The Ministry of Information Technology was formed in 1999 burdened with the enormous duty of making India an IT super power by 2008. In less than a year, India witnessed the enactment of its first statute relating to information technology[1] on the pattern of the Model Law on Electronic Commerce, 1996, adopted by the United Nations Commission on International Trade Law. The Electronic Transactions Act, 1998 of Singapore also significantly guided the framing of the Act. The Information Technology Act, 2000 was passed by Parliament on May 15, 2000, approved by the President on June 9, 2000 and notified to come into force on October 17, 2000.

The Information Technology Act intends to give legal recognition to e-commerce and e-governance and facilitate its development as an alternate to paper based traditional methods. The Act has adopted a functional equivalents approach in which paper based requirements such as documents, records and signatures are replaced with their electronic counterparts. The Act seeks to protect this advancement in technology by defining crimes, prescribing punishments, laying down procedures for investigation and forming regulatory authorities. Many electronic crimes have been bought within the definition of traditional crimes too by means of amendment to the Indian Penal Code, 1860. The Evidence Act, 1872 and the Banker's Book Evidence Act, 1891 too have been suitably amended in order to facilitate collection of evidence in fighting electronic crimes.

1.4.1 A Quick Overview of the Act

Section 1 deals with the extent, commencement and application of the Act. It also specifically prohibits the application in certain situations. Section 2 of the Act deals with definitions. Digital Signature has been vastly covered under Chapters II, VI, VII and VIII. Chapters III and IV exclusively deal with electronic records. Chapter V introduces the concept of secure electronic records and secure digital signatures as also the security procedure. Offences and Penalties under the Act have been enumerated in Chapters IX and XI whereas the Cyber Regulations Appellate Tribunal, its constitution, powers and functions have been laid down in Chapter X. Chapter XII deals with the issue of liability of network service providers. Finally, Chapter XIII deals with residuary matters like police powers, removal of difficulties, power to make rules and regulations, amendment to various enactments, etc. There are four Schedules to the Act each dealing with amendments to the four enactments indicated above. This is the span of the Act. In the following discussion, though relevant definitions would be given either in the running paragraphs, or in the footnotes, still, for quick reference, the reader is advised to refer to section 2 of the IT Act and the Glossary given in Schedule V of the Information Technology (Certifying Authorities) Rules. A detailed discussion of the Act is attempted in the next two units.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

Discuss the salient features of the Information Technology Act, 2000.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

1.5 CRITIQUES OF THE I.T. ACT

The IT Act, 2000 came at a time when cyber-specific legislation was much needed. Moreover India was one of the earliest countries to draft a legislation of this kind. Without a doubt, the IT Act has not only helped India achieve the position that it holds today in the IT sector but also helped overseas based IT

and related investors gather a favourable impression of India's IT related legal system, and therefore make a decision to invest in India. While a lot can be said the merits of the Act, there is room for some improvement too.

One of the main drawbacks of the Act seems to be its inadequacy in providing sufficient data protection provisions. With the transformation of the Internet into the main arena of conduct of economic activities, there is a danger of the possibility of key data being the target of crooks, for snooping paparazzi, for espionage agencies etc.

The IT Act does not offer much in terms of protection of intellectual property on the net. In other words there are no provisions in the act to protect copyrights, patents or trademarks. To take a more specific example, the Act has no provisions to deal with what is known as 'cyber squatting' relating to domain name disputes. Though the area is presently covered laws relating to intellectual property like Trade Marks, it is desirable for the IT Act also to have such a provision. For instance when a major company wishes to register a domain name in lets say .in, and it suddenly finds someone else wholly unconnected to the company having registered the name of the company in that category, the company has no remedy under the IT Act though it has the trademark for that name. Similarly, there are no provisions in the IT Act to address cyber theft, cyber stalking, cyber defamation etc.

On privacy issues also the Act has come in for a lot of flak. It does not prohibit behaviour like spams and unsolicited e-mails that flood one's in-box. Neither does it provide for instances where there is a misuse of confidential private data collected online.

The IT Act also is silent on issues relating to cross border taxation arising out of international trade, which in the long run is inevitable and would turn out to be a contentious issue.

Even from the purely technological standpoint there is a criticism that the Act binds digital signatures to the asymmetric encryption system, limiting the scope of innovation in technology. This is a drawback given the fact that technology is constantly changing with one system giving place to another.

A single section devoted to liability of the Network Service Provider is highly inadequate. The issues are many more. Apart from classification of the Network Service Providers itself, there are various instances in which the Provider can be made liable especially under other enactments like the Copyright Act or the Trademark Act. However, the provision in the IT Act, 2000 devoted to ISP protection against any liability is restricted only to the Act or rules or regulations made thereunder. The section (though it might be argued the other way round, still) is not very clear as to whether the protection for the ISPs extends even under the other enactments.

There has been a general criticism of the wide powers given to the police under the Act. Fear, especially among cyber café owners, regarding misuse of powers under the IT Act, 2000 is not misplaced. Anyone can be searched and arrested without any warrant at any point of time in a public place. But at the

same time, the fact that committing a computer crime over the net and the possibility of escaping thereafter is so much more viable, that providing such policing powers to check the menace of computer crimes is also equally important. Again, interception of electronic messages and e-mails might be necessary under certain situations but the authorities cannot be given a free-hand in interception as and when they feel. Similarly, we need to enquire and delve deeper into police powers of investigation, search and warrant under the IT Act, 2000 and look for a more balanced solution.

Another criticism of the Act seems to be that offences can be prosecuted both under the civil and the criminal procedure system. Some of the instances that provide for fine would have to be taken as per provisions of the civil procedure code which is generally perceived to be a slow process. Other offences that involve punishments of imprisonment would be as per the provisions of the Criminal Procedure Code.

Finally, how the Act will be interpreted by a court of law and its implementation and flaws in the long run are yet to be tested on a case-specific factual terrain as the number of cases that have come before the higher courts under the Act is just a handful.

1.6 PROPOSED AMENDMENTS TO THE I.T. ACT

With an objective to review the Information Technology Act 2000, in the light of the latest developments and to consider the feedback received for removal of certain deficiencies, an expert committee under the Chairmanship of Shri. Brijesh Kumar, Secretary, Department of Information Technology was set up. The committee had during its deliberations analysed some of the relevant experiences and international best practices. The Committees recommendations have been with the twin objectives of using the IT as a tool for socio-economic development and employment generation, and also to further consolidate India's position as a major global player in the IT sector.

As the technologies and applications in IT sector change very rapidly, some of the provisions related parameters that may change from time to time have been proposed to be amended to provide for the new developments to be incorporated by changes in rules/govt notifications. This would enable law to be amended and approved much faster and would keep our laws in line with the changing technological environment. The Act is proposed to be made technology neutral with minimum change in the existing IT Act 2000. One major change proposed is the substitution of "digital signature" with "electronic signature" through an amendment to section 4. Digital signature is thus recognised as one of the types of electronic authentication of records and not as the only way. This is more in the nature of an enabling provision so as to include more forms of authentication as and when technology advances. Further in order to allow public-private partnership in e-governance delivery of services, certain amendments have been proposed.

A new chapter (III A) under the title "Electronic Contracts" is proposed to be added with section 10 proposing to give validity to Electronic Contracts. Another impetus to e-commerce is sought to be given through this amendment.

In view of the concerns about the operating provisions in the IT Act related to data protection and privacy, in addition to contractual agreements between parties, the existing Sections, for instance 43, 65, 66 and 72 have been revisited and some amendments have been proposed.

A new section is being added (Sec 67(2)) to address child pornography with higher punishment and fine of global standards. So also now a new form of illegal conduct called video voyeurism, which means capturing the private area of an individual without his/her consent and then transmitting it, has been included as punishable conduct.

With regards to the use of encryption and also with relation to interception and monitoring and decryption of any information, provisions that have a bearing on national security, some changes based on the recommendation of the Ministry of Home Affairs as well as the Inter Ministerial Working Group on Cyber Laws and Cyber Forensics has been proposed.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

Critically examine the amendments suggested by the Brijesh kumar committee.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

1.7 SUMMARY

- With the phenomenal growth of information and communication technology and its importance in development it was soon realised that the field had to be regulated. Regulation of a technological advancement bought in technology based laws, principally the IT Act.
- In this connection laws can be categorised into two classes—

1) Laws may be technology neutral such as laws relating to defamation, forgery, contract company etc. Here it is immaterial whether activities covered by these acts are performed on the Internet or not.

2) Laws relating to the activities which can be performed on the Internet only such as hacking, denial of services, viruses etc.

- Cyber laws in the domestic field consist of the IT Act supplemented by a wide number of other Acts.
- The Act gives legal recognition to e-commerce, e-governance, digital signature keeping records in electronic form etc. It also defines crimes relating to computer and Internet and makes provisions for their investigation and makes provision for punishment.
- We have also seen that the IT Act has a lot of scope for improvement and that an amendment is already in the cards. The expert committee set up by the government has suggested making the Act more technology neutral. Some of the amendments suggested by the committee are — replacement of the word — digital signature by electronic signature, making provision for electronic contract, child pornography, etc.

1.8 TERMINAL QUESTIONS

1) Discuss the need of special laws in the field of cyberspace? Do you think that Indian laws sufficiently deal with every aspect of the challenges posed by the technology in the field of cyberspace?

1.9 ANSWERS AND HINTS

1. Phenomenal growth in the use of Internet in almost every walk of life has posed the challenge of regulating the cyberspace. Such as identity of the person, electronic signature in the contract and other transactions on the Internet, hacking, virus etc. therefore special legal provisions are needed to cope with it.

   Indian IT Act has tried to address these issues but more needs to be done. Government set up a committee to suggest amendment in the act. Committee maid valuable suggestions which should be incorporated in any future amendment to the Act.

2) Section 1 deals with the extent, commencement and application of the Act. It also specifically prohibits the application in certain situations. Section 2 of the Act deals with definitions. Digital Signature has been vastly covered under Chapters II, VI, VII and VIII. Chapters III and IV exclusively deal with electronic records. Chapter V introduces the concept of secure electronic records and secure digital signatures as also the security procedure. Offences and Penalties under the Act have been enumerated in Chapters IX and XI whereas the Cyber Regulations Appellate Tribunal, its constitution, powers and functions have been laid down in Chapter X. Chapter XII deals with the issue of liability of network service providers. Finally, Chapter XIII deals with residuary matters like police powers, removal of difficulties, power to make rules and regulations, amendment to various enactments, etc. There are four Schedules to the Act each

dealing with amendments to the four enactments indicated above. This is the span of the Act. In the following discussion, though relevant definitions would be given either in the running paragraphs, or in the footnotes, still, for quick reference, the reader is advised to refer to section 2 of the IT Act and the Glossary given in Schedule V of the Information Technology (Certifying Authorities) Rules. A detailed discussion of the Act is in the next two units.

3) With an objective to review the Information Technology Act 2000, in the light of the latest developments and to consider the feedback received for removal of certain deficiencies, an expert committee under the Chairmanship of Shri. Brijesh Kumar, Secretary Department of Information Technology was set up. The committee had during its deliberations analysed some of the relevant experiences and international best practices. The Committees recommendations have been with the twin objective of: using the IT as a tool for socio-economic development and employment generation, and also to further consolidate India's position as a major global player in the IT sector.

   A new chapter (III A) under the title "Electronic Contracts" is proposed to be added with section 10 proposing to give validity to Electronic Contracts. Another impetus to e-commerce is sought to be given through this amendment.

   In view of the concerns about the operating provisions in the IT act related to data protection and privacy, in addition to contractual agreements between parties, the existing Sections for instance 43, 65, 66 and 72 have been revisited and some amendments have been proposed. A new section is being added (Sec 67(2)) to address child pornography with higher punishment and fine of global standards. So also now a new form of illegal conduct called video voyeurism, which is capturing the private area of an individual without his consent and then transmitting it, has been included as a punishable conduct.

1.10 REFERENCES AND SUGGESTED READINGS

Under the Act, the following rules, regulations and guidelines have been framed: (a) the Information Technology (Certifying Authorities) Rules, 2000; (b) the Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000; (c) the Information Technology (Certifying Authority) Regulations, 2001; and, (d) the Guidelines for Submission of Application for Certifying Authority, 2001.

UNIT 2 INFORMATION TECHNOLOGY ACT – PART I

Structure

2.1 INTRODUCTION

In the previous unit we have tried to present a broad picture of the IT Act. In the next two units, we shall examine the provisions of the Information Technology Act, 2000 in detail. In this unit we shall discuss the objectives for which this Act has been passed. This unit will also discuss the extra-territorial application of the Act. This has become important because computer related wrongs know no boundaries. A wrongful act committed in one country may affect the computers and computer networks of not only the country where the wrong has been committed but also of other countries.

The IT Act has introduced certain new concepts such as “digital signature” “e-governance” etc. The Act gives legal recognition to the electronic records and treat its at par with the paper based system if all the safeguards are followed.

2.2 OBJECTIVES

After studying this unit you should be able to:

- discuss the aims and objectives of the Act i.e. what does the Act try to achieve?

- analyse the concept of digital signature and discuss the powers and functions of the issuing authorities a authority to exercise control over the issuance of digital signatures; and
- discuss the provisions relating to e-governance and legal recognition of electronic records.

2.3 STATEMENT OF OBJECTS AND REASONS

The statement of objects and reasons of the IT Act reflects the purpose of the enactment and what it is trying to achieve. The concern of the framers of the IT Act was the need for information to be collected, stored and utilized in electronic form which in turn would serve the dual purpose of facilitating e-commerce and inducting e-governance in the system.

Another object was clearly aimed at giving effect to the United Nations General Assembly Resolution[1] whereby the Model Law on Electronic Commerce was adopted by the United Nations Commission on International Trade Law. It recommended the States to give a favourable consideration to the Model Law when they enact or revise their laws, '*in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information*'. Thus, the idea has been to make a shift from the paper-based system to electronic system whereby the communication and storage of data would be through the electronic medium rather than on paper.

The solution devised is by giving a statutory mechanism to the creation and use of digital signatures in the country. For this purpose, the required institution is created which would be responsible for issuance of Digital Signature Certificates and subsequent verification so that it can be used in e-commerce and e-governance. Certain 'deeming' provisions have been incorporated to supplement the existing laws and support them for the electronic era. The Act attempts to achieve the need of e-governance by providing for e-records. It provides a statutory support to electronic records so that they can be used for promotion of efficient delivery of government services.

Cyber crimes have been dealt with by providing for punishment for certain computer-related wrongs. Finally, the Act also provides for electronic transfer of funds. Various other Acts namely the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Reserve Bank of India Act, 1934 and the Bankers' Books Evidence Act, 1891 have been suitably amended to suit the electronic era.

2.4 APPLICATION OF THE ACT – THE EXTRA-TERRITORIAL EFFECT

The application of the Act and its extra-territorial effect can be well understood by a conjoint reading of **sections 1, 75 and 81**. The Act extends to the whole of India.[2] It applies also to any offence or contravention thereunder committed outside India by any person. However, an exception to this rule has been carved out in section 75 of the Act. Sub-section (1) of section 75 though in wider terms has made the Act applicable also to any offence or contravention committed outside India by any person irrespective of his nationality, this sub-

section has been made subject to the provisions of sub-section (2) which states that for the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person, if the act or conduct constituting the offence or contravention *involves* a computer, computer system or computer network in India. In effect, if an act (amounting to an offence under the Act) has been committed and where any computer, computer system or computers which are interconnected to each other in a computer network and which is in India is also involved (which might be either as a tool for committing the crime or as a target to the crime), then the provisions of the Act would apply to such an act. Section 81 provides effect to the provisions of the Act notwithstanding anything inconsistent contained in any other law for the time being in force. Therefore, effectively even if an offence (falling under the Act) is committed outside India by a foreigner, yet the courts in India would have the jurisdiction.

It is noticeable that with the IT Act, there has been a conceptual change with regard to the applicability of a statute. Due to the borderless connectivity of the computers through the Internet, and the ease with which one can commit a cyber crime in India while physically located beyond the boundaries of the country, the Parliament has made the provisions of the Act applicable irrespective of where the accused might be physically located. In contrast, if we see the extent of operation of the Indian Penal Code (IPC) under section 1,[3] it extends only 'to the whole of India except the State of Jammu and Kashmir'. No further applicability clause has been provided for. Section 2 of the IPC makes every person including a foreigner liable to punishment for every act or omission contrary to the provisions of IPC, of which he/she shall be guilty in India. Sections 3 and 4 of the IPC relate to the extra-territorial operation of the Code. But these sections too are restrictive in nature and not as broad as the combined effect of section 1(2) read with section 75 of the IT Act.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

Discuss the extra-territorial effect of the IT Act. In what respect are its provisions are different from I.P.C.?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2.5 DIGITAL SIGNATURES (CHAPTERS II, V, VI, VII, VIII)

Before we start discussing the topic of digital signature under the IT Act we must bear in mind that the expert committee to review the IT Act (discussed in the previous chapter) has proposed one major change that is the substitution of “digital signature” with “electronic signature” through an amendment to section 4. Digital signature is thus recognised as *one* of the types of electronic signature only. Therefore, very soon all references to digital signature in the IT Act may be substituted with electronic signature.

Any commercial transaction necessarily requires an agreement between two parties. For having a more secure transaction, people prefer having the agreement written and signed. With the advent of information technology and movement of the business on the Internet, it became necessary that there should be a secure form of entering into online contracts. In an online environment, the same is done through digital signatures.

Affixing a digital signature implies the electronic authentication of an electronic document. It has a two-fold purpose: (a) identification of the person who is signing the document; (b) authentication of the contents of the document which is being signed. In the Act, Chapters II, VI, VII and VIII are devoted to digital signatures. In these chapters have been laid down the mechanism for issuance, modification and revocation of digital signatures, the authorities who would be assigned the task related to digital signatures, their powers and functions, and the duties of the subscribers of the digital signatures.

The whole system creates a hierarchy in which at the top of is the Controller of Certifying Authorities who has the power to appoint Certifying Authorities and grant them the licence to issue Digital Signature Certificates. In turn, the Certifying Authorities can issue such Certificates to the subscribers. The process of application, renewal, suspension and revocation of licence of the Certifying Authorities has been provided. Likewise, the power to issue, suspend and revoke digital signature certificates is given in the hands of the Certifying Authorities. A hierarchy of digital signature certificates too has been provided for the purpose of verification of genuineness of digital signatures which ultimately can be verified by the Controller of Certifying Authorities who under the Act is the highest authority for digital signatures and related matters.

Section 2(p) of the Act defines ‘digital signature’ as ‘authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3’. Chapter II of the Act has a single section that is section 3 providing for authentication of electronic records. Sub-section (1) of section 3 states that ‘any subscriber may authenticate an electronic record by affixing his digital signature’. This forms the base of use of digital signature. Section 3(1) of the Act gives a legal sanctity to the usage of digital signatures in the country. A person can, if he/she wishes, use digital signatures to authenticate an electronic record and such authentication is now recognisable under the law.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

What is digital signature and what purpose is achieved by it?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2.5.1 Controller of Certifying Authorities

At the top of the hierarchy of authorities under the Act for the purpose of issuance of digital signature certificates is the Controller of the Certifying Authorities. Under Section 17(1) of the Act, the Central Government has been empowered to appoint a Controller for the purposes of the Act.

The functions of the Controller have been enumerated under section 18 of the Act. These functions basically relate to Certifying Authorities or Digital Signature Certificate. It is the Controller's duty to regulate and control almost each and every activity of the Certifying Authorities. This is particularly important since the primary work of the Certifying Authorities is issuance of digital signatures and setting up infrastructure for its subsequent public verification. The Controller also has the function of specifying the form and content of a Digital Certificate and the key as also specifying the contents of written, printed, or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key. In case of conflict of interests between the Certifying Authorities and the subscribers, the Controller has been empowered to resolve the same.

Controller to act as Repository

Under section 20 of the Act, the Controller has been made the repository of all Digital Signature Certificates issued under the Act. The responsibility of the secrecy and security of the Certificates is on the Controller who shall make use of appropriate hardware, software and procedures that are secure from intrusion and misuse. The Controller is also under an obligation to

maintain a computerised database of all public keys in such a manner that such database and the public keys are available to any member of the public.

Recognition of Foreign Certifying Authorities

Section 19 of the Act gives the power to the Controller to recognise any Certifying Authority for the purposes of the Act subject to certain conditions.

Power to investigate contraventions

Section 28 empowers the Controller to take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

Directions to extend facilities to decrypt information

The Controller has, under sub-section (1) of section 69, the power to direct any agency of the Government to intercept any information transmitted through any computer resource. However, certain conditions have been laid down, which have to be fulfilled before such power can be exercised.

i) The Controller should be satisfied that such interception is necessary in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence.

ii) Such reasons must be recorded in writing.

iii) The direction to the agency must be by an order.

2.5.2 Licence to Issue Digital Signature Certificates

An elaborate discussion has been made in the Act with regard to the licence to issue Digital Signature Certificates. The provisions of the Act cover the application for licence, grant or rejection of licence, renewal of licence, suspension of licence, display of licence and surrender of licence. The Controller has been made the sole authority with regard to all these activities.

2.6 E-GOVERNANCE (CHAPTER III)

Chapter III covers the area of legal recognition of certain paper-based concepts and functions in electronic form. Sections 4 to 8 provide for legal recognition of electronic records, digital signatures, use of electronic records and digital signatures in Government and its agencies, retention of electronic records, and publication of rule, regulation, etc. in Electronic Gazette. This Chapter serves a dual purpose: (a) it introduces the principle of functional equivalence; and, (b) it provides the foundation to one of the averred objects of the Act of introducing e-governance by ‘facilitating electronic filing of documents with the government agencies’.

2.6.1 Functional-Equivalent Approach

Chapter III of the Act has adopted the ‘functional-equivalent’ approach. This approach is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or

functions could be fulfilled through electronic-commerce techniques. When adopting this approach in the UNCITARL Model Law, attention was given to the existing hierarchy of form requirements, which provides distinct level of reliability, traceability and inalterability with respect to paper-based documents. This approach singles out the basic functions of paper-based form requirements, with a view to providing criteria which, once they are met by electronic documents, enable such e-documents to enjoy the same level of legal recognition as corresponding paper documents performing the same function enjoy. For example, if a contract is signed and sent as an electronic document, the chances of its reliability would be, in general situations, lesser than that of a paper-based document due to certain doubts as to its authenticity and chances of alteration of the contents. However, if the same electronic document is sent after being digitally signed by using a digital signature certificate issued by a trustworthy digital signature certificate provider, then, since it would be able to perform the same *functions* of reliability, traceability and inalterability as a paper-based document, it would receive legal sanction. What is noticeable is that a document in electronic form can, with suitable technical guards, perform the functions of writing much better than a paper-based document.

For the purpose of this Chapter, definition of 'electronic form', as provided under section 2(r) of the Act, is very material. It means, with reference to information, any information generated, sent, received, or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

What is the functional equivalent approach? Discuss whether the electronically produced data with suitable technical safe-guard is as reliable, traceable and unalterable as the data written on paper.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2.6.2 Legal Recognition of Electronic Records

Section 4[4] of the Act deems the fulfillment of the requirement of any information to be in writing in typewritten or printed form, if such information fulfills two conditions. Firstly, such information should be rendered or made available in an electronic form (for example, in a floppy disk). Secondly, such information is accessible as to be usable for a subsequent reference. The word 'accessible', as per the UNCITRAL guide, is meant to imply that information in the form of computer data should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained. The word 'usable' is not intended to cover only human use but also computer processing. 'Subsequent reference' seems to imply merely the need for future reference. The carefully worded section does not seem to lay down any stringent standards as to the reliability or durability of the electronic record. Rather, it merely requires that such information if made available at a certain point of time in electronic form should be available for usage at some future time as well. The purpose is to basically provide a legal sanctity to production of any information in electronic form. Whether such information provided is correct, or authentic, or unaltered, or reliable is not within the purview of this section. If the law provides something to be in writing, then, subject to certain conditions, the legal requirement of writing would be fulfilled if such information is in electronic form.

2.6.3 Legal Recognition of Digital Signatures

Section 5[5] proceeds on the functional-equivalent approach. It is based on the recognition of the functions of a signature in a paper-based environment. The following functions of a signature are considered in the UNCITRAL Guide[6]: (a) identifying a person; (b) providing certainty as to the personal involvement of that person in the act of signing; (c) associating such person with the content of the document.[7] Broadly, these being the functions of a signature, the purpose of section 5 is to merely introduce and give legal sanctity and acceptance to the use of digital signatures. It is not necessary as to what is the mode of signature; it may be paper-based or electronic. However, so long as the functions of the signature are being performed, such signature will receive legal recognition. Section 5 of the Act states that where any law provides that any information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government. The Explanation to the Section further clarifies the ambit of the word 'signature' as to mean, 'with its grammatical variations and cognate expressions, with reference to a person, affixed of his hand written signature or any mark on any document'. Section 5, like section 4, has a limited field of operation. It is not the purpose of section 5 to ascertain whether the digital signature affixed is as per the rules prescribed, or whether the functions of a signature have been fulfilled. The purpose is merely to provide legal recognition to a digital signature on par with hand-written signature wherever the law requires the affixation of such signature.

2.6.4 Use of Electronic Records and Digital Signatures in Government and its Agencies

Section 6 provides for use of electronic records and digital signatures in government functioning. If any particular law requires filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government[8] in a particular manner, or the issuance or grant of any licence, permit, sanction or approval by whatever name called in a particular manner, or the receipt or payment of money in a particular manner, then, under sub-section (1) of the section 6, such requirement would be deemed to have been satisfied if such filing, issue, grant, receipt or payment, is effected by means of an electronic form. Such electronic form may be prescribed by the appropriate government. The appropriate government, under sub-section (2), has been given the power to make rules to prescribe the manner and format in which such electronic records shall be filed, created or issued, as also the manner or method of payment of any fee or charges for filing, creation or issuance of any electronic record.

Therefore, an application for a document say, a land record, if made in the prescribed electronic form to the revenue and land records department, it would be legally valid under section 6. Or, a grant of certificate of registration as a dealer by the government under a sales tax legislation in an electronic form is now legally recognisable.

2.6.5 Retention of Electronic Records

Various statutes provide for storage of information (for example, for tax purposes or auditing/accounting, etc.). Such information is generally stored on paper-based mode. However, with increase in computers for processing and storage of information, it became imperative to provide legal sanction to storage of information in electronic form. Modern trade works through information technology and requires it to retain all the information, though generated, sent or received in electronic form, in paper-based mode would be a step back. Section 7 of the Act permits retention of information in electronic form and gives legal recognition to retention of electronic records. Where any law provides that documents, records of information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in electronic form. The section deems the fulfillment of the legal requirement of paper-based retention of information if the same is done in electronic form.

2.7 SUMMARY

- In this unit we have examined in detail the objects and reasons for the IT Act, the applicability of the Act i.e. the extra territorial application of the Act, provisions relating to digital signatures, e-commerce and e-governance. This part of the IT Act deals with the recognition of the electronic record and its legalisation as an alternative to paper based records.

- The aim of the Act is to give legal recognition to the information collected, stored and utilized in electronic form so as to facilitate electronic commerce and e-governance.
- The Act gives legal recognition to digital signature and provides for the issuance, of it. It also provides for the controlling mechanism to check abuse of digital signature.
- The Act provides for the appointment of the controller of the certifying authority who shall issue licences to the authorities who can issue digital signatures. The Controller has also been granted powers to recognise foreign certifying authorities in this respect.
- The Act adopts the functional equivalent approach i.e. if the electronic records satisfy the same level of reliability as the paper document, it should be given the same recognition as the paper based record.

2.8 TERMINAL QUESTIONS

1) What is digital signature? How is it issued? Discuss the powers and functions of the controller of certifying authority and the certifying authorities.
2) What is the functional equivalent approach? Discuss how it is adopted in the Act with respect to the digital signature and electronic records. Do you think that the electronic records satisfy the test of reliability, traceability and inalterability in the same way as the paper based records?
3) What are the conditions of the recognition of electronic record? Do you think that the provisions contained in the Act adequately deal with the issue?

2.9 ANSWERS AND HINTS

1) The application of the Act and its extra-territorial effect can be well understood by a conjoint reading of **sections 1, 75 and 81**. The Act extends to the whole of India. It applies also to any offence or contravention thereunder committed outside India by any person. However, an exception to this rule has been carved out in section 75 of the Act. Sub-section (1) of section 75 though in wider terms has made the Act applicable also to any offence or contravention committed outside India by any person irrespective of his nationality, this sub-section has been made subject to the provisions of sub-section (2) which states that for the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person, if the act or conduct constituting the offence or contravention *involves* a computer, computer system or computer network in India. In effect, if an act (amounting to an offence under the Act) has been committed and where any computer, computer system or computers which are interconnected to each other in a computer network and which is in India is also involved (which might be either as a tool for committing the crime or as a target to the crime), then the provisions of the Act would apply to such an act. Section 81 provides effect to the provisions of the Act notwithstanding anything inconsistent

contained in any other law for the time being in force. Therefore, effectively even if an offence (falling under the Act) is committed outside India by a foreigner, yet the courts in India would have the jurisdiction.

It is noticeable that with the IT Act, there has been a conceptual change with regard to the applicability of a statute. Due to the borderless connectivity of the computers through the Internet, and the ease with which one can commit a cyber crime in India while physically located beyond the boundaries of the country, the Parliament has made the provisions of the Act applicable irrespective of where the accused might be physically located. In contrast, if we see the extent of operation of the Indian Penal Code (IPC) under section 1, it extends only 'to the whole of India except the State of Jammu and Kashmir'. No further applicability clause has been provided for. Section 2 of the IPC makes every person including a foreigner liable to punishment for every act or omission contrary to the provisions of IPC, of which he shall be guilty in India. Sections 3 and 4 of the IPC relate to the extra-territorial operation of the Code. But these sections too are restrictive in nature and not as broad as the combined effect of section 1(2) read with section 75 of the IT Act.

2) Affixing the digital signature implies the electronic authentication of an electronic document. It performs the same function as the signature by hand. The Act makes provision for the appointment of a Controller of Certifying Authorities that is empowered to grant licences to authorities who may issue digital signatures. The Act makes elaborate provisions in this regard.

3) Functional equivalent approach in the context of electronic signature and records mean that they perform similar functions as the signature by hand and paper based documents. If these are done with adequate safeguards, they are more reliable than their traditional counterparts.

2.10 REFERENCES AND SUGGESTED READINGS

1. Resolution no. A/RES/51/162. 30 Jan.1997.
2. S. 1(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.
3. S. 1. – This Act shall be called the Indian Penal Code, and shall extend to the whole of India except the State of Jammu and Kashmir.
4. S. 4. Legal recognition of electronic records. Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—
   a) rendered or made available in an electronic form; and
   b) accessible so as to be usable for a subsequent reference.

5. S. 5. Legal recognition of digital signatures. Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

6. Para. 53 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996).

7. *Explanation.* — For the purposes of this section, "*signed*", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "*signature*" shall be construed accordingly.

8. S. 2(e). – 'appropriate Government' means as respects any matter, - (I) enumerated in List II of the Seventh Schedule to the Constitution; (ii) relating to any law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government.

UNIT 3 INFORMATION TECHNOLOGY ACT – PART II

Structure

3.1 INTRODUCTION

In the previous unit you have seen that various new concepts such as digital signature, e-governance, functional equivalent approach etc. have been introduced by the IT Act, 2000. The first unit of this block gave you some idea as to what types of challenges are faced by the legal system due to the advancement of information technology.

You may have understood the fact that these challenges require different types of adjudicatory mechanism and different types of offences and penalties to be incorporated in law because the existing law cannot deal adequately with these issues.

In this unit we shall discuss the adjudicatory mechanism provided in the IT Act. We shall also discuss the offences and penalties provided in the Act and how the offences under the Act be investigated. The investigation of IT related offences is a very complicated affair. In these types of investigations special kind of investigation techniques are applied.

The Act also amends certain provisions of Indian Penal Code, Indian Evidence Act etc. The objective of these amendments is to enlarge the definitions of certain offences so as to include within them the commission of these offences electronically and give legal recognition to evidence of electronic records.

While studying this unit it is recommended that apart from the copy of the IT Act, 2000, you should also keep the copies of the IPC, 1860 and Indian Evidence Act, 1872 with you for having a glance at the bare provisions of these Acts to understand the true scope of this unit.

3.2 OBJECTIVES

After studying this unit, you should be able to:

- discuss the powers, functions and qualifications and what procedure is to be followed by the adjudicating officer and C.R.A.T., and discuss the penalties and offences in case of the contravention of the Act;
- define the term and discuss network service provider and his/her liabilities for offences committed using his/her network. What are the circumstances under which he/she may be exempted from such liabilities?
- describe amendments made by this Act in different statutes to give legal recognition to the electronically kept document, enlarge the definitions of certain offences to include within them the commitment of offences electronically and transfer of fund electronically.

3.3 ADJUDICATION (CHAPTER IX)

The Act provides for its own adjudicating mechanism and procedure. It appoints adjudicating officers conferring on them powers to adjudicate upon any allegations of contravention of the provisions of the Act or rules or regulations made thereunder. It also constitutes a Cyber Regulations Appellate Tribunal (CRAT) for the purpose of hearing appeals arising out of decisions of the adjudicating officer as also the Controller under various provisions of the Act.

3.3.1 Adjudicating Officer

Section 46 of the Act provides for appointment, powers and functions of the adjudicating officer. Under sub-section (1), the Central Government shall appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer. Such adjudicating officers should possess such experience in the field of Information Technology and legal or judicial experience as prescribed by the Central Government. The adjudicating officer is required to hold an inquiry and thereafter, adjudge whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made there under. If, after providing such opportunity and on the basis of inquiry made under sub-section (1), the adjudicating officer is satisfied that the person has committed the contravention, then, he/she may impose such penalty or award such compensation as he/she thinks fit in accordance with the provisions of that section.

3.3.2 Cyber Regulations Appellate Tribunal

Chapter X of the Act contains provisions relating to Cyber Regulations Appellate Tribunal (CRAT). The Central Government by notification will establish one or more appellate tribunals to be known as Cyber Regulations Appellate Tribunal (CRAT). The Central Government will also in such notification specify the matters and places in relation to which the CRAT may exercise jurisdiction. CRAT will consist of one person only ('the Presiding Officer') to be appointed by the Central Government, by notification.

Presiding Officer of CRAT

For appointment as a Presiding Officer of CRAT, a person will not be qualified unless he/she (a) is, or has been, or is qualified to be, a Judge of a High Court; or, (b) is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

Appeal to and Procedure and Powers of the CRAT

The Central Government in exercise of its rule-making power under section 87 of the Act framed the Cyber Regulations Appellate Tribunal (Procedure) Rules, 200[1] regulating the procedure to be followed in applications made to the CRAT.

Section 57 of the Act provides for appeal to the CRAT. Sub-section (1) gives the right to appeal to any person who is aggrieved by the order of the Controller or an adjudicating officer under this Act to CRAT having jurisdiction in the matter. However, this right is subject to the provisions of sub-section (2) which prohibits any appeal against any order of an adjudicating officer made with the consent of the parties.

The appeal shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.[2] As regards the procedure to be followed during an appeal, Section 58 of the Act provides that CRAT is not bound by the procedure laid down by the Code of Civil Procedure, 1908. However, it shall be guided by the principles of natural justice. Sub-section (2) of section 58 provides that the CRAT has the same powers as are vested in a civil court under the Code of Civil Procedure, 1908.

Section 61 of the Act bars the jurisdiction of all other courts to entertain any suit or proceeding in respect of any matter which an adjudicating officer or the CRAT is empowered under this Act to determine. The section further provides that no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred under this Act.

Section 62 of the Act provides for an appeal to the High Court against the order of the CRAT. Such appeal can be made on any question of fact or law arising out of the order appealed against. The scope, therefore, of interference in the order of the CRAT by the High Court is quite wide.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

Give a brief account of the powers and functions of the adjudicating officer and the CRAT.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

3.4 PENALTIES AND OFFENCES (CHAPTER IX & XI)

Penalties and offences are dealt with in different Chapters in the Act. Chapter IX, which also harbours provisions relating to adjudication, enumerates the various penalties and the entailing civil consequences. Chapter XI deals exclusively with offences.

3.4.1 Penalties

Three kinds of conduct have been listed out in the Act which would give rise to civil consequences. Firstly, any person involved in any action relating to damage to computer, computer system, etc., under section 43 of the Act, would be liable to damages. Second group pertains to failure to furnish information, returns, etc. under section 44. And finally section 45 contains the residuary clause.

Section 43 of the Act provides a list of activities which, if carried out by any person without the permission of the owner or any other person who is in charge of a computer, computer system or computer network, would cause such person who is carrying out the act to be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. Such activities include:

A) Accessing or securing access to a computer, computer system or computer network. This in effect refers to unauthorized access.

B) Downloading, copying or extracting any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium. This means data theft and would also include acts of copyright infringement like downloading of music.

C) Introducing or causing to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.

D) Damaging or causing to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network.

E) Disrupting or causing disruption of any computer, computer system or computer network.

F) Denying or causing the denial of access to any person authorized to access any computer, computer system or computer network by any means.

G) Providing any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under. This is a facet of hacking.

H) Charging the services availed of by a person to the account of another person by tampering with or manipulation any computer, computer system or computer network. This refers to theft of Internet hours.

Confiscation of computer, computer system, floppies, compact disks, tape drives or any other accessories in respect of which of any provision of this Act, rules, orders or regulations has been or is being contravened, can be resorted to under section 76.

3.4.2 Offences

Chapter XI of the Act enumerates the various acts which constitute an offence under the Act along with the punishment be it either imprisonment or fine or both. Such offences:

In case of offences committed by companies, such persons who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, will be, under sub-section (1) of section 85 of the Act, guilty of the contravention and shall be liable to be proceeded against and punished accordingly. However, if such person proves that the contravention took place without his/her knowledge or that he/she exercised all due diligence to prevent such contravention, he/she shall not be liable to punishment. Sub-section (2) of section 85 also deems a director, manager, secretary or any other officer of the company to be guilty of contravention and liable for punishment if it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of such person. ‘Company’, for the purpose of this section, has been explained to mean any body corporate and includes a firm or other association of individuals. ‘Director’, in relation to a firm, would mean a partner in the firm.

3.4.3 Investigation

Section 78 of the Act places the powers of investigation with a police officer not below the rank of Deputy Superintendent of Police. This provision overrides anything contrary in the Code of Criminal Procedure. Section 80 confers the powers on police officers to enter and search premises.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

Discuss the provisions of the IT Act 2000 relating to the penalty and punishment.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

3.5 NETWORK SERVICE PROVIDER LIABILITY (CHAPTER XII)

The issue of Network Service Provider has gained importance with the increase of offences being committed via the Internet especially in the area of copyright infringement. They are being held up for abetting the offence by providing infrastructural facilities which help the offender to commit the offence. However, to provide immunity to them, section 79 of the Act provides for certain cases where they will not be liable. In case of any allegation of liability under the Act, rules or regulations against a Network Service Provider for any third party information or data made available by him/her, he/she shall not be liable if he/she proves that the offence or contravention was committed without his/her knowledge or that he/she had exercised all due diligence to prevent the commission of such offence or contravention. ‘Network service provider’, for the purpose of this section, has been explained to mean an intermediary. ‘Third party information’ is given to mean any information dealt with by a network service provider in his/her capacity as an intermediary.

To take an example, if A is hacking B's computer and using the network services provided by Z, a network service provider, then, to the extent that Z is able to prove that the offence was committed without his/her knowledge or that he/she had exercised all due diligence to prevent the commission of such offence, he/she will be saved from any liability by virtue of section 79 of the Act. However, what is worth taking note of is that the burden of proof has been shifted to the network service provider. It would not be very difficult for someone to just pull any network service provider into litigation and then burdening him with the task of proving due diligence and commission without knowledge. Keeping in mind the number of litigations that might ensue due to contraventions based on the Internet, the task for network service providers has really been reduced and immunity provided can still be burdensome. Alternatively, the initial burden of proving that enough communication was given to the network service provider should lie on the complainant. Thereafter, the onus could shift to the network service provider that there was no knowledge or that due diligence was exercised.

3.6 AMENDMENTS TO CERTAIN STATUTES

The Act, to further the acceptance and use of documents, evidence, and transfer of funds through electronic means, has amended the Indian Penal Code, Indian Evidence Act, Bankers' Books Evidence Act and Reserve Bank of India Act vide the First, Second, Third and Fourth Schedule respectively. As the Act proposes such heavy induction of use of electronic means for documents and signatures, as also governance, it became necessary to also amend certain penal statutes to bring it on par with the offences relating to or committed with the help of such electronic means. Many of such offences have already been enumerated in the Act itself. However, such offences relate to a new category which has emerged with the use of computer technology like hacking, damage to computer systems, etc. There is another set of offences which were already on the statute books but with the use of electronic means have taken a new dimension and their scope needs to be further widened by appropriate amendments in such statutes. This is what the amendments made by the Act purport to achieve.

3.6.1 Amendments to the Indian Penal Code, 1860

Certain provisions of the Indian Penal Code (IPC) have been amended by Section 91. These provisions primarily are offences relating to document. The aim is to also include 'electronic record' thereby including such offences which till now were only paper-based but can now also be paperless. For example, for the purpose of forgery, it is no more necessary that the document forged has to be signed (which traditionally would require a signature of a person on a paper-based document) but has now been extended to forgery by affixing a digital signature as well.

Largely, the amendments to the IPC can be categorised under five headings:

a) *Definition*: By insertion of section 29A, the definition of 'electronic record' as understood by section 2(1) (t) of the Act has been introduced in the IPC.

b) *Offences by or relating to public servants*: Section 167 deals with the offence committed by a public servant of framing an incorrect document with intent to cause injury. The amendment makes the public servant liable to punishment for the offence even in case of framing, preparation or translation of an electronic record.

c) *Offences of contempt of the lawful authority of public servants*: Chapter 10 of IPC deals with contempt of the lawful authority of public servants and is meant to enforce obedience and respect to their lawful authority. All the amendments made in this Chapter pertain to introduction of 'electronic record' by the side of 'document' and bringing on par both paper-based and paperless offences. Sections 172,[3] 173[4] and 175[5] have been amended to ensure that any action which was done by way of a paper-based document would still be an offence if done by way of electronic means.

d) *Offences relating to evidence*: Sections 192[6] and 204[7] have been amended under the Chapter relating to offences of false evidence and offences against public justice. After the amendments, the offence of fabricating false evidence would also include fabricating of a false electronic record. Likewise, any destruction of an electronic record would attract punishment under section 204.

e) *Offences in relation to document*: The major portion of the amendments made in the IPC is dedicated to the Chapter 18 that is offences relating to documents. All such offences pertaining to and based on the document have been given a wider scope and are applicable to electronic records as well. Such amendments primarily relate to use of electronic record and affixation of digital signatures for the purpose of forgery. Section 463 which makes forgery a punishable offence has been amended to include forgery by electronic record. Making of a false document under section 464 now includes dishonestly or fraudulently affixing any digital signature on any electronic record. 'Affixing digital signature' has been given the same meaning as assigned to it in section 2(1) (d) of the Act. Sections 466,[8] 468,[9] 470,[10] 471[11] and 474[12] have been amended to the same effect that is committing forgery by electronic record and affixing digital signature.

3.6.2 Amendments to the Indian Evidence Act, 1872

Section 92 of the Act amends certain provisions of the Evidence Act. These amendments can be summarized under four headings:

a) *Amendments permitting evidence in electronic form*: The definition of 'documentary evidence' under section 3 of the Evidence Act has been amended to include 'electronic records' as well. The definitions of 'certifying authority', 'digital signature', 'digital signature certificate', 'electronic form', 'electronic records', 'information', 'secure electronic record', secure digital signature and 'subscriber' have been inserted and are to have the same meaning as assigned to them in the IT Act. Section 17 of the Evidence Act dealing with the definition of admission now

includes a statement contained in electronic form as well. Sections 34[13] and 35[14] have been amended to include documents maintained in electronic form and electronic record respectively. Section 39 dealing with the evidence to be given when statement forms part of a conversation, document, book or series of letters or papers has been appropriately amended to include within its gamut 'electronic records'. Section 59 states that 'all facts except the contents of documents may be proved by oral evidence'. The amendment now permits proving of all facts by oral evidence except contents of document or electronic records. Therefore, one cannot by oral evidence prove the contents of an electronic record. Section131[15] has been amended to include any person in possession of an electronic record. The purpose of these amendments seems to basically inculcate the concept of evidence through electronic records. It creates a base for the amendments mentioned herein below. This set of amendments does not pertain to the questions of genuineness of the electronic records being produced as evidence or issues relating to their evidentiary value. The only object is to be able to produce evidence in electronic form in a court.

b) *Expert opinion on digital signatures*: Section 47A has been inserted whereby the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact[16] when the court has to form an opinion as to the digital signature of any person.

c) *Amendments relating to evidentiary value and evidence*: Certain amendments by way of insertions have been made by the IT Act in the Evidence Act to introduce electronic evidence in the Indian legal system. Such electronic evidence has been permitted by use of electronic records before a court of law. Section 3 as noted above was amended to include electronic records within the definition of evidence. In continuation to this amendment, certain further amendments have been made permitting electronic records to be evidence. As to what should be the rules to test the acceptability and genuineness of such electronic records as evidence has been introduced by these amendments. Section 22A relates to the relevance of oral admissions as to the contents of an electronic record unless the genuineness of the electronic record produced is in question. Section 65A and 65B collectively form the base for proving the contents of an electronic record. Sections 67A and 73A relate to proving and verification of digital signature respectively.

d) *Presumptions*: Introduction of evidence through electronic records has also led to certain additional presumptions under the Evidence Act. Section 81A provides for presumption of genuineness of Gazettes in electronic form. Certain presumptions have been provided for under sections 85A, 85B and 85C relating to electronic agreements, electronic records and digital signatures, and digital signature certificates. Section 85C relates to presumption with respect to electronic messages and section 90A with regard to presumption as to electronic records which are purported or proved to be five years old.

Please answer the following Self Assessment Question.

Self Assessment Question 3 & 4 *Spend 6 Min.*

Discuss in brief the amendment made by the IT Act, 2000 in the IPC. What is the objective behind these amendments?

Discuss the amendments made by the IT Act, 2000 in the Evidence Act, 1872. What is the purpose of this amendment?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

3.7 SUMMARY

In this unit we have discussed the adjudicatory mechanisms provided in the IT Act, 2000. We have also discussed the offences and penalties provided for in the Act including the liability of the service providers. Finally we have also examined the amendments made by the IT Act, 2000 in the Indian Penal Code, 1860 and Indian Evidence Act, 1872. The purpose of these amendments is to redefine various offences so as to include the commission of these offences electronically and to give the electronic records the same evidentiary value as the paper based documents.

3.8 TERMINAL QUESTIONS

1) Discuss the powers, functions and procedure for the adjudication of disputes under the IT Act, 2000.

2) What amendments has been made in the Indian Penal Code, 1860 and Indian Evidence Act, 1872 by the I.T. Act? What is the purpose of these amendments?

3.9 ANSWERS AND HINTS

1) The Act provides for the appointments of the adjudicating officers and cyber regulation appellate tribunals to settle the disputes relating to the offences and penalties provided in the act.

2) Three kinds of conduct have been listed out in the Act which would give rise to civil consequences. Firstly, any person involved in any action relating to damage to computer, computer system, etc., under section 43 of the Act, would be liable to damages. Second group pertains for failure to furnishing of information, returns, etc. under section 44. And finally section 45 contains the residuary clause.

Section 43 of the Act provides a list of activities which, if carried out by any person without the permission of the owner or any other person who is in charge of a computer, computer system or computer network, would cause such person who is carrying out the act to be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. Such activities include:

A) Accessing or securing access to a computer, computer system or computer network. This in effect refers to unauthorized access.

B) Downloading, copying or extracting any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium. This means data theft and would also include acts of copyright infringement like downloading of music.

C) Introducing or causing to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.

D) Damaging or causing to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network.

E) Disrupting or causing disruption of any computer, computer system or computer network.

F) Denying or causing the denial of access to any person authorized to access any computer, computer system or computer network by any means.

G) Providing any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under. This is a facet of hacking.

H) Charging the services availed of by a person to the account of another person by tampering with or manipulation any computer, computer system or computer network. This refers to theft of Internet hours.

Confiscation of computer, computer system, floppies, compact disks, tape drives or any other accessories in respect of which any provision of this Act, rules, orders or regulations has been or is being contravened, can be resorted to under section 76.

Offences

Chapter XI of the Act enumerates the various acts which constitute an offence under the Act along with the punishment be it either imprisonment or fine or both. Such offences:

In case of offences committed by companies, such persons who, at the time the contravention was committed, was in charge of, and was responsible, to, the company for the conduct of business of the company as well as the company, will be, under sub-section (1) of section 85 of the Act, guilty of the contravention and shall be liable to be proceeded against and punished accordingly. However, if such person proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention, he shall not be liable to punishment. Sub-section (2) of section 85 also deems a director, manager, secretary or any other office of the company to be guilty of contravention and liable for punishment if it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of such person. 'Company', for the purpose of this section, has been explained to mean any body corporate and includes a firm or other association of individuals. 'Director', in relation to a firm, would mean a partner in the firm.

3 & 4) The objective of the amendments in the various statutes by this act is to give same status to the electronic records and signature as the paper based documents and signature underhand.

3.10 REFERENCES AND SUGGESTED READINGS

1. *Vide* G.S.R. 791 (E). 17 Oct. 2000.
2. S. 57(6) of the IT Act, 2000.
3. S. 172 of the Indian Penal Code. - Absconding to avoid service to summons or other proceedings.
4. S. 173 of the Indian Penal Code. - Preventing service of summons or other proceeding, or preventing publication thereof.
5. S. 175 of the Indian Penal Code. - Omission to produce document to public servant by person legally bound to product it.
6. S. 192 of the Indian Penal Code. - Fabricating false evidence.
7. S. 204 of the Indian Penal Code. - Destruction of document to prevent its production as evidence.
8. S. 466 of the Indian Penal Code. - Forgery of record of Court or of public register, etc.
9. S. 468 of the Indian Penal Code. - Forgery for purpose of cheating.
10. S. 470 of the Indian Penal Code. - Forged document.
11. S. 471 of the Indian Penal Code. - Using as genuine a forged document.

12. S. 474 of the Indian Penal Code. - Having possession of document described in S. 466 or 467, knowing it to be forged and intending to use it as genuine.

13. S. 34 of the Evidence Act. - Entries in books of account when relevant.

14. S. 34 of the Evidence Act. - Relevance of entry in public record, made in performance of duty.

15. S. 131 S. 34 of the Evidence Act. - Production of documents or electronic records which another person, having possession, could refuse to produce.

16. This has an important bearing keeping in mind S. 5 of the Evidence Act which states that, ‘Evidence may be given in any suit or proceeding of the existence or non-existence of every fact in issue and of such other facts as are hereinafter declared to be relevant, and of no others.’

UNIT 4 INTERNATIONAL TREATIES, CONVENTIONS AND PROTOCOLS CONCERNING CYBERSPACE

Structure

4.1 INTRODUCTION

After discussing domestic law in the previous three units, in this unit we shall discuss the international instruments and institutions dealing with cyber law and cyberspace. These are also integral parts of the legal system because the challenges posed by ICT are of universal nature, hence they cannot be addressed by one country alone without international cooperation.

The laws of cyber laws constitute the laws and regulations administered by national institutions together with the ones administered by international, intergovernmental and international non governmental organizations. Several International agencies are active in matters relating to the regulation of cyberspace and the media through which they execute these regulations are international legal instruments like treaties, agreements, conventions, charters, protocols, declarations, memoranda of understanding, modus vivendi and exchange of notes. In fact, the meaning of the terms used to describe an international instrument is variable, changing from State to State, from region to region and instrument to instrument. Some of the terms can easily be interchanged: an instrument that is designated “agreement” might also be called “treaty”. The 1969 Vienna Convention on the Law of Treaties is the principal law governing the international law of rights and obligations that treaties entail. In this chapter we shall discuss some of the important international instruments that have a bearing on the global cyber law regime and as a natural corollary we shall also examine the work of the international organizations that are the custodians of these instruments.

4.2 OBJECTIVES

After studying this unit you should be able to:

- discuss the efforts made internationally to facilitate the growth and accessibility of Information and Communication Technology; and
- examine the role played by the international organizations and agencies to give electronic records the same recognition as paper based documents.

4.3 UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW

The most prominent among all the international organizations is the United Nations. The United Nations Commission on International Trade Law (UNCITRAL) is the agency charged with the responsibility of harmonization and unification of International trade laws. Based in Vienna, UNCITRAL is a legal body with universal membership specialising in commercial law reform worldwide for over 40 years. UNCITRAL's business is the modernisation and harmonisation of rules on international business.

With the growing usage of electronic commerce and advanced communications technology in international trade, the UNCITRAL came up with a Model Law on Electronic Commerce in 1996. This was based on a Resolution of the General Assembly of the United Nations of 1985[1], urging governments and international organizations to take action to ensure legal security in the context of the widest possible use of automated data processing in international trade. This model law was adopted by the UNCTRAL in the Commission's twenty-ninth session after observations of governments and other interested organizations. One of the guiding factors during the drafting of the model law was that the law should facilitate the use of electronic commerce that is acceptable to states with different legal, social and economic systems so as to significantly contribute to the development of harmonious international economic relations. The model law was intended to assist all states in framing appropriate legislation governing the usage of alternatives to paper-based methods of communication and storage of information.

Following the framing of the Model Law the United Nations General Assembly by its Resolution No. 51/62, dated 30th January 1997[2], recommended that all states should give favourable consideration to the said law when they frame or revise their own law. The model law with its provision for equal treatment of users of electronic communications and paper based communication soon became the basis of several national legislations including the Information Technology Act of 2000 of India.

Currently the UNCITRAL in 2005 came out with the United Nations Convention on the Use of Electronic Communications in International Contracts. This was adopted by the General Assembly on 23 November 2005; the Convention aims to enhance legal certainty and commercial predictability where electronic communications are used in relation to international contracts. It addresses the determination of a party's location in an electronic environment;

the time and place of dispatch and receipt of electronic communications; the use of automated message systems for contract formation; and the criteria to be used for establishing functional equivalence between electronic communications and paper documents — including "original" paper documents — as well as between electronic authentication methods and hand-written signatures. This instrument is now open for countries to sign and ratify.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

Discuss the efforts made by the UNCITRAL in the development of cyber law? Did it influence in any manner the Indian law in this area?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

4.4 WORLD SUMMIT ON INFORMATION SOCIETY

Under the aegis of the United Nations, with the International Telecommunication Union playing a key role, a World Summit on Information Society (WSIS) was held in two phases in Geneva, from1-12 December 2003 and in Tunis, from 16-18 November 2005. At the summit in Geneva in 2003, world leaders realising the immense potential of information and communication technologies in human development, declared their "common desire and commitment to build a people-centered, inclusive and development oriented information society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights." One objective of the WSIS was to address the uneven distribution of the benefits of the information technology revolution between the developed and developing countries and within societies, what is known as the digital divide.

A Plan of Action was adopted in Geneva to give effect to the vision of an inclusive information and communication society aimed at bridging the digital divide and building digital solidarity. The targets that were laid down in the action plan to be achieved by 2015 by all nations are listed below.

a) to connect villages with ICTs and establish community access points;

b) to connect universities, colleges, secondary schools and primary schools with ICTs;

c) to connect scientific and research centres with ICTs;

d) to connect public libraries, cultural centres, museums, post offices and archives with ICTs;

e) to connect health centers and hospitals with ICTs;

f) to connect all local and central government departments and establish websites and e-mail addresses;

g) to adapt all primary and secondary school curricula to meet the challenges of the Information Society, taking into account national circumstances;

h) to ensure that all of the world's population have access to television and radio services;

i) to encourage the development of content and to put in place technical conditions in order to facilitate the presence and use of all world languages on the Internet;

j) to ensure that more than half the world's inhabitants have access to ICTs within their reach.

At the summit held in 2005 in Tunisia, governments reaffirmed their dedication to the commitments made in Geneva and decided to further build on them focusing on financial mechanisms for bridging the digital divide and also on areas such as internet governance as well as follow up on Geneva and Tunis decisions. A Tunis Agenda for the Information Society was adopted along with a Tunis Commitment that outlined the basis for the implementation and follow-up of the Agenda. The agenda has further identified the strategy to meet the obligations of the Geneva plan. There the agenda proposes to undertake efforts for:

a) mainstreaming and aligning national e-strategies, across local, national, and regional action plans, as appropriate and in accordance with local and national development priorities, with in-built time-bound measures.

b) developing and implementing enabling policies that reflect national realities and promote a supportive international environment, foreign direct investment as well as the mobilisation of domestic resources, in order to promote and foster entrepreneurship, particularly Small, Medium and Micro Enterprises (SMMEs), taking into account the relevant market and cultural contexts. These policies should be reflected in a transparent, equitable regulatory framework to create a competitive environment to support these goals and strengthen economic growth.

c) building ICT capacity for all and confidence in the use of ICTs by all – including youth, older persons, women, indigenous peoples, people with

disabilities, and remote and rural communities – through the improvement and delivery of relevant education and training programmes and systems including lifelong and distance learning.

d) implementing effective training and education, particularly in ICT, science and technology that motivates and promotes participation and active involvement of girls and women in the decision-making process of building the Information Society.

e) paying special attention to the formulation of universal design concepts and the use of assistive technologies that promote access for all persons, including those with disabilities.

f) promoting public policies aimed at providing affordable access at all levels, including community-level, to hardware as well as software and connectivity through an increasingly converging technological environment, capacity building and local content.

g) improving access to the world's health knowledge and telemedicine services, in particular in areas such as global cooperation in emergency response, access to and networking among health professionals to help improve quality of life and environmental conditions.

h) building ICT capacities to improve access and use of postal networks and services.

i) using ICTs to improve access to agricultural knowledge, combat poverty, and support production of and access to locally relevant agriculture-related content.

j) developing and implementing e-government applications based on open standards in order to enhance the growth and interoperability of e-government systems, at all levels, thereby furthering access to government information and services, and contributing to building ICT networks and developing services that are available anywhere and anytime, to anyone and on any device.

k) supporting educational, scientific, and cultural institutions, including libraries, archives and museums, in their role of developing, providing equitable, open and affordable access to, and preserving diverse and varied content, including in digital form, to support informal and formal education, research and innovation; and in particular supporting libraries in their public-service role of providing free and equitable access to information and of improving ICT literacy and community connectivity, particularly in underserved communities.

l) enhancing the capacity of communities in all regions to develop content in local and/or indigenous languages.

m) strengthening the creation of quality e-content, on national, regional and international levels.

n) promoting the use of traditional and new media in order to foster universal access to information, culture and knowledge for all people, especially vulnerable populations and populations in developing countries and using, inter alia, radio and television as educational and learning tools.

o) reaffirming the independence, pluralism and diversity of media, and freedom of information including through, as appropriate, the development of domestic legislation, we reiterate our call for the responsible use and treatment of information by the media in accordance with the highest ethical and professional standards. We reaffirm the necessity of reducing international imbalances affecting the media, particularly as regards infrastructure, technical resources and the development of human skills. These reaffirmations are made with reference to Geneva Declaration of Principles paragraphs 55 to 59.

p) strongly encouraging ICT enterprises and entrepreneurs to develop and use environment-friendly production processes in order to minimize the negative impacts of the use and manufacture of ICTs and disposal of ICT waste on people and the environment. In this context, it is important to give particular attention to the specific needs of the developing countries.

q) incorporating regulatory, self-regulatory, and other effective policies and frameworks to protect children and young people from abuse and exploitation through ICTs into national plans of action and e-strategies.

r) promoting the development of advanced research networks, at national, regional and international levels, in order to improve collaboration in science, technology and higher education.

s) promoting voluntary service, at the community level, to help maximize the developmental impact of ICTs.

t) promoting the use of ICTs to enhance flexible ways of working, including teleworking, leading to greater productivity and job creation.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

Discuss the principles enunciated in the WSIS summits.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

4.5 UNITED NATIONS COMMISSION ON TRADE AND DEVELOPMENT

United Nations Commission on Trade and Development (UNCTAD) is the United Nations General Assembly's main agency responsible for trade and development. Since 1998 when the General Assembly gave UNCTAD a special grant to pursue and develop electronic commerce initiatives, this agency has been active in its advocacy of the role and importance of information and communication technologies in development.

UNCTAD carries out policy-oriented analytical work on the *information economy* and its implications for developing countries. Its analytical work is published in the annual *Information Economy Report* (former E-commerce and Development Report). It also assists governments, businesses and civil society groups that are considering adopting *free and open source software* policies.

UNCTAD has also published the *Digital Divide: ICT Development Indices 2004,* which benchmarks ICT diffusion for over 150 countries using indices of connectivity and access. It also monitors trends in ICT development to raise awareness and helps formulate policies aimed at narrowing the digital divide.

4.6 COUNCIL OF EUROPE

Council of Europe is an *international organization* of 46 member states in the *European* region. The Council is most prominent for the *European Convention on Human Rights 1950*, which serves as the basis for the *European Court of Human Rights*. The Council of Europe is not to be confused with the *Council of the European Union* or the *European Council*, as it is a separate organization and not part of the *European Union.*

The Council was set up to:

- Defend human rights, parliamentary democracy and the rule of law
- Develop continent-wide agreements to standardise member countries' social and legal practices,

The Council of Europe came out with a Convention on Cyber crime (2001) and its additional Protocol concerning the acts of a racist and xenophobic nature committed through computer systems (2003). The Convention aims principally at: (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form and (3) setting up a fast and effective regime of international co-operation.

The Convention contains four chapters: (I) Use of terms; (II) Measures to be taken at domestic level – substantive law and procedural law; (III) International co-operation; (IV) Final clauses.

Section 1 of Chapter II (substantive law issues) covers both criminalization provisions and other connected provisions in the area of computer- or computer-related crime: it first defines 9 offences grouped in 4 different categories, then deals with ancillary liability and sanctions. The following offences are defined by the Convention: illegal access, illegal interception, data interference, and system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights.

Section 2 of Chapter II (procedural law issues) – the scope of which goes beyond the offences defined in section 1 in that it applies to any offence committed by means of a computer system or the evidence of which is in electronic form – determines first the common conditions and safeguards, applicable to all procedural powers in this Chapter. It then sets out the following procedural powers: expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data; real-time collection of traffic data; interception of content data. Chapter II ends with the jurisdiction provisions.

Chapter III contains the provisions concerning traditional and computer crime-related mutual assistance as well as extradition rules. It covers traditional mutual assistance in two situations: where no legal basis (treaty, reciprocal legislation, etc.) exists between parties – in which case its provisions apply – and where such a basis exists – in which case the existing arrangements also apply to assistance under this Convention. Computer- or computer-related crime specific assistance applies to situations and covers, subject to extra-conditions, the same range of procedural powers as defined in Chapter II. In addition, Chapter III contains a provision on a specific type of transporter access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Parties.

4.7 WORLD TRADE ORGANIZATION

The growing importance of electronic commerce in global trade led World Trade Organization (WTO) members to adopt a *declaration on global electronic commerce* on 20 May 1998 at their Second Ministerial Conference in Geneva, Switzerland. The Declaration directed the WTO General Council to establish a comprehensive *work programme* to examine all trade-related issues arising from electronic commerce, and to present a progress report to the WTO's Third Ministerial Conference.

The 1998 declaration also included a so-called moratorium stating that "members will continue their current practice of not imposing customs duties on electronic transmission".

The work programme was adopted by the WTO General Council on 25 September 1998. It continued after the Third Ministerial Conference in Seattle in November 1999.

At the Fourth Ministerial Conference in Doha in 2001, ministers agreed to continue the work programme as well as to extend the moratorium on customs

duties. They instructed the General Council, in *paragraph 34 of the Doha Declaration*, to report on further progress to the Fifth Ministerial conference at Cancún, in 2003.

Under the work programme, issues related to electronic commerce have been examined by the Council for Trade in Services, the Council for Trade in Goods, the Council for TRIPS and the Committee on Trade and Development. During the course of the work programme a number of background notes on the issues have been produced by the WTO Secretariat and many member governments have submitted documents outlining their own thoughts.

After the Doha Ministerial Declaration, the General Council agreed to hold "dedicated" discussions on cross-cutting issues, i.e. issues whose potential relevance may "cut across" different agreements of the multilateral system. So far, there have been five discussions dedicated to electronic commerce, held under the General Council's auspices.

The issues discussed included: classification of the content of certain electronic transmissions; development-related issues; fiscal implications of e-commerce; relationship (and possible substitution effects) between e-commerce and traditional forms of commerce; imposition of customs duties on electronic transmissions; competition; jurisdiction and applicable law/other legal issues.

Participants in the dedicated discussions hold the view that the examination of these crosscutting issues is unfinished, and that further work to clarify these issues is needed.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

Discuss the salient features of WTO Declaration on Global Electronic Commerce.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

4.8 WORLD INTELLECTUAL PROPERTY ORGANIZATION

WIPO, the Geneva based World Intellectual Property Organization has a world-wide coverage with179 member states. The purpose of WIPO is to "to promote the protection of intellectual property throughout the world through cooperation among states". (Art. 3 WIPO Convention). WIPO is the forum for international IP policy making, development and administration of the 23 international treaties of which it is the custodian.

Migration of intellectual property to the digital world, IP being ideally suited to digitization, is the order of the day. IP on the net is vulnerable because infinite number of perfect copies can be made and easily distributed through digital networks worldwide. There is therefore understandably a need to protect internet content including information, music, software, films, business methods, databases, etc.

Among the IP Issues on the Internet, the problem of the abusive registration of trademarks as domain names known in other words as cyber squatting is one of the areas that the WIPO addresses. The WIPO works through Uniform Domain Name Dispute Resolution Policy adopted by ICANN, and provides the services of a Domain name registrar. It also provides for alternative dispute resolution services through its Arbitration and Mediation center.

Significant issues in the field of copyright have been examined for a number of years through various public and private processes, at WIPO and other international organizations, and at national and regional levels. Significant progress has been made, with international consensus having already emerged on some of these issues. In 1996, two treaties were adopted by consensus by more than 100 countries at WIPO: the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) (commonly referred to as the "Internet Treaties"). The treaties, each having reached their 30th ratification or accession, both have entered into force: the WCT on March 6, 2002, and the WPPT on May 20, 2002.

The WIPO Internet Treaties are designed to update and supplement the existing international treaties on copyright and related rights, namely, the Berne Convention and the Rome Convention. They respond to the challenges posed by the digital technologies and, in particular, the dissemination of protected material over the global networks that make up the Internet. The contents of the Internet Treaties can be divided into three parts: (1) incorporation of certain provisions of the TRIPS Agreement not previously included explicitly in WIPO treaties (e.g. protection of computer programs and original databases as literary works under copyright law); (2) updates not specific to digital technologies (e.g., the generalized right of communication to the public); and (3) provisions that specifically address the impact of digital technologies.

Although the Internet Treaties have now entered into force, in order that they are truly effective in the digital environment, they must become widely adopted in countries around the world, and their provisions must be incorporated in national legislation.

There have also been some regulations from other intergovernmental bodies like the European Union and also by international non-governmental bodies like international chambers of Commerce.

4.9 SUMMARY

Cyber laws also include all the international instruments governing cyberspace. Therefore in this chapter we have examined some important international treaties, bodies international instruments formulated by various international organizations such as the United Nations Commission on International Trade Law (UNCITRAL), the work of the World Summit on Information Society (WSIS), the United Nations Commission on Trade and Development (UNCTAD), Council of Europe, World Trade Organization (WTO) and the World Intellectual Property Organization (WIPO).

The objectives of these international organizations are to give equal status to electronic documents with the paper based documents, to connect government departments, health centers, universities and other educational and research organizations via Internet thus to promote e-governance, to make the computer and internet accessible to all irrespective of the economic status etc, to encourage the development of software in regional languages so that every section of the society may be benefited by the information and communication technology, to encourage the development devices and software for the persons with disabilities so that they may also be benefited by the ICT revolution etc.

4.10 TERMINAL QUESTION

1) Discuss the steps taken by international organizations to make Information and Communication Technology universally accessible.

4.11 ANSWERS AND HINTS

1) With the growing usage of electronic commerce and advanced communications technology in international trade, the UNCITRAL came up with a Model Law on Electronic Commerce in 1996. This was based on a Resolution of the General Assembly of the United Nations of 1985, urging governments and international organizations to take action to ensure legal security in the context of the widest possible use of automated data processing in international trade. This model law was adopted by the UNCTRAL in the Commission's twenty-ninth session after observations of governments and other interested organizations. One of the guiding factors during the drafting of the model law was that the law should facilitate the use of electronic commerce that is acceptable to states with different legal, social and economic systems so as to significantly contribute to the development of harmonious international economic relations. The model law was intended to assist all sates in framing appropriate legislation governing the usage of alternatives to paper-based methods of communication and storage of information.

2) Under the aegis of the United Nations, with the International Telecommunication Union playing a key role, a World Summit on Information Society (WSIS) was held in two phases in Geneva, 1-12 December 2003 and in Tunis, 16-18 November 2005. In Geneva in 2003, world leaders realising the immense potential of information and communication technologies in human development, declared their "common desire and commitment to build a people-centered, inclusive and development oriented information society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights." Amongst the objectives of the of the WSIS was to address the uneven distribution of the benefits of the information technology revolution between the developed and developing countries and within societies, what is known as the digital divide.

A Plan of Action was adopted in Geneva to give effect to the vision of an inclusive information and communication society aimed at bridging the digital divide and building digital solidarity. The targets that were laid down in the action plan to be achieved by 2015 by all nations are listed below.

a) to connect villages with ICTs and establish community access points;

b) to connect universities, colleges, secondary schools and primary schools with ICTs;

c) to connect scientific and research centres with ICTs;

d) to connect public libraries, cultural centres, museums, post offices and archives with ICTs;

e) to connect health centers and hospitals with ICTs;

f) to connect all local and central government departments and establish websites and e-mail addresses;

g) to adapt all primary and secondary school curricula to meet the challenges of the Information Society, taking into account national circumstances;

h) to ensure that all of the world's population have access to television and radio services;

i) to encourage the development of content and to put in place technical conditions in order to facilitate the presence and use of all world languages on the Internet;

j) to ensure that more than half the world's inhabitants have access to ICTs within their reach.

3) The growing importance of electronic commerce in global trade led World Trade Organization (WTO) members to adopt a *declaration on global electronic commerce* on 20 May 1998 at their Second Ministerial Conference in Geneva, Switzerland. The Declaration directed the WTO General Council to establish a comprehensive *work programme* to examine all trade-related issues arising from electronic commerce, and to present a progress report to the WTO's Third Ministerial Conference.

4.12 REFERENCES AND SUGGESTED READINGS

1. 40/71 of 11 Dec. 1985 (A/40/17).
2. A/RES/51/162. 30 Jan.1997.

UNIT 5 GUIDELINES ISSUED BY VARIOUS MINISTRIES

Structure

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.