Comparative Sections:
Senator Karim Khuwaja's and Government's Proposed Bills

Below are sections that are similar in terms of the definitions, offences, procedures and powers outlined in both bills. However, the language and detail in which they exist, and their scope, varies.

Senator Karim Khuwaja's Proposed Bill	Government's Proposed Bill
1. Short title, extent, application and commencement.- (1) This Act may be called the Protection of Cyber Crimes Act, 2014. (2) It extends to the whole of Pakistan. (3) The provisions of this Act applies where- (a) an offence under this Act was committed in Pakistan; (b) any act of preparation towards an offence under this Act or any part of the offence was committed in Pakistan or where any result of the offence has had an effect in Grenada; (c) an offence under this Act was committed by a Pakistani national or a person resident or carrying out business in Pakistan or visiting Pakistan or staying in transit in Pakistan; (d) an offence under this Act was committed in relation to or connected with an electronic system or data in Pakistan or capable of being connected, sent to, used by or with an electronic system in Pakistan; or (e) an offence under this Act was committed by any person, of any nationality or citizenship or in any place outside or inside Pakistan, having an effect on the security of Pakistan or its nationals, or having universal application	1. Short title, extent, application and commencement.- (1) This Act may be called the Prevention of Electronic Crimes Act, 2015. (2) It extends to the whole of Pakistan. (3) It shall apply to every citizen of Pakistan wherever he may be, and also to every other person for the time being in Pakistan. (4) It shall come into force at once.

under international law, custom and usage. (4) It shall come into force at once.	
Chapter 1 Definitions	**Chapter 1 Definitions**
(a) "Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network; **(b) "access to program or data"** means access to any program or data held in any information systems if by causing an information system to perform any function whereby a person — (i) alters, modifies or erases the program or data or any aspect or attribute related to the program or data; or (ii) copies, transfers or moves it to any information system, device or storage medium other than that in which it is held; or to a different location in the same information system, device or storage medium in which it is held; or (iii) uses it; or (iv) has it output from the information system in which it is held, whether by having it displayed or in any other manner: Provided that for the purposes of paragraph (b) (iii) above a person uses a program if the function he causes the information system to perform causes the program to be executed; or is itself a function of the program: Provided further that for the purposes of paragraph (b) (iv) above a program is output if the instructions of which it consists are output; and the form in which	**(b) "access to data"** means gaining control or ability to read, use, copy, modify or delete any data held in or generated by any device or information system; **(c) "access to information system"** means gaining control or ability to use any part or whole of an information system whether or not through infringing any security measure;

any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by an information system) is immaterial;	
(h) "Computer System" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions; **(s) "electronic device"** is any hardware that accomplishes its functions using any form or combination of electrical energy;	**(o) "device"** includes- (i) physical device or article; (ii) any electronic or virtual tool that is not in physical form; (iii) a password, access code or similar data, in electronic or other form, by which the whole or any part of an information system is capable of being accessed; or (iv)automated, self-executing, adaptive or autonomous devices, programs or information systems; **(s) "information system"** means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information;
(d) "Code" means the Code of Criminal Procedure, 1898 (V of 1898);	**(g) "Code"** means the Code of Criminal Procedure, 1898 (V of 1898);
(j)"critical infrastructure" means the assets, systems and networks, whether physical or virtual, so vital to the State that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof;	**(j) "critical infrastructure"** includes: (i) the infrastructure so vital to the State or other organs of the Constitution such that its incapacitation disrupts or adversely affects the national security, economy, public order, supplies, services, health, safety or matters incidental or related thereto or (ii) any other private or Government infrastructure so designated by the Government as critical infrastructure as per rules prescribed under this Act;
(k) "critical infrastructure information system, program or data" means any	**(k) "critical infrastructure information system or data"** means an information

information system, program or data that supports or performs a function with respect to a critical infrastructure;	system, program or data that supports or performs a function with respect to a critical infrastructure;
(m) "damage" includes modifying, altering, deleting, erasing, suppressing, changing location or making data temporarily unavailable, halting an electronic system or disrupting the networks;	**(l) "damage to an information system"** means any unauthorised change in the ordinary working of an information system that impairs its performance, access, output or change in location whether temporary or permanent and with or without causing any change in the system; (n) "data damage" means alteration, deletion, deterioration, erasure, relocation, suppression, of data or making data temporarily or permanently unavailable; **(n) "data damage"** means alteration, deletion, deterioration, erasure, relocation, suppression, of data or making data temporarily or permanently unavailable;
(n) "data" includes representations of facts, information or concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including electronic program, text, images, sound, video and information within a database or electronic system;	**(m) "data"** includes content data and traffic data;
(o) "Decryption" means the process of transforming or unscrambling encrypted data from its unreadable and incomprehensible format to its plain version; **(zc) "plain version"** means original data before it has been transformed or scrambled to an unreadable or incomprehensible format;	**Section 32: Explanation.-** Decryption information means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable form and from ciphered data to intelligible data.

(q) "electronic" means relating to technology having electrical, digital, magnetic, optical, biometric, electrochemical, wireless, electromagnetic, or similar capabilities;	**(p) "electronic"** includes electrical, digital, magnetic, optical, biometric, electrochemical, electromechanical, wireless or electromagnetic technology;
(x) "information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;	**(r) "information"** includes text, message, data, voice, sound, database, video, signals, software, computer programs, any form of intelligence as defined under the Pakistan Telecommunication (Reorganization) Act, 1996 and codes including object code and source code;
(y) "malicious code" means an electronic program or a hidden function in a program that infects data with or without attaching its copy to a file and is capable of spreading over an electronic system with or without human intervention including virus, worm or Trojan horse;	**Section 20: Explanation.-** For the purpose of this section the expression "malicious code" includes a computer program or a hidden function in a program that damages an information system or data or compromises the performance of such system or availability of data or uses it without proper authorisation.
(za) "Password" means a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information;	**(q) "identity information"** means an information which may authenticate or identify an individual or an information system and enable access to any data or information system;
(ze) "service provider" means– (i) a person who provides an information and communication service including the sending, receiving, storing or processing of the electronic communication or the provision of other services in relation to it through an electronic system; (ii) a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunications services; or (iii) any other person that processes or stores data on behalf of such electronic	**(aa) "service provider"** includes a person who: (i) acts as a service provider in relation to sending, receiving, storing, processing or distribution of any electronic communication or the provision of other services in relation to electronic communication through an information system; (ii) owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; (iii) processes or stores data on behalf of such electronic communication service or users of such service; or

communication service or users of search service;	(iv)provides premises from where or facilities through which the public in general may access the Internet against payment of charges for the same;
(zf) "Special Court" means the Court of Sessions competent to try offences under this Act;	**(i) "Court"** means the Court of competent jurisdiction designated under this Act;

(zh) "subscriber information" means any information contained in any form that is held by a service provider, relating to subscribers of its services other than traffic data and by which can be established– (i) the type of communication service used, the technical provisions taken thereto and the period of service; (ii) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or (iii) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement;	**(bb) "subscriber information"** means any information held in any form by a service provider relating to a subscriber other than traffic data;
(zj) "traffic data" means any data relating to a communication by means of an electronic system, generated by an electronic system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service; and	**(cc) "traffic data"** includes data relating to a communication indicating its origin, destination, route, time, size, duration or type of service;
(zk) "unauthorized access" means access of any kind by a person to an electronic system or data held in an electronic system which is unauthorized or done without authority or is in excess	**(dd)"unauthorised access"** means access to such information system or data which is not available for access by general public, without authorisation or in

of authority, if the person is not himself entitled to control access of the kind in question to the electronic system or data and the person does not have consent to such access from a person so entitled.	violation of the terms and conditions of the authorisation;
Chapter IV Offences and Punishments	**Chapter II Offences and Punishments**
54. Illegal Entree to Information System.- Whoever with intent to unauthorized entree or secures entree to such electronic system, computer or perform function unlawfully on an information system whole or any part of such electronic system, computer or an information system shall be punished with imprisonment of either for a term which may extend to nine months or with fine which may extend to two hundred thousand rupees or with both. 55. Illegal Entree to Program or Data.- Whoever unlawfully, whether temporarily or not with intent causes access to any program or data to be secured or to be enabled, download, copy or extract data, electronic database or information from such electronic system or network including information or data held or stored in a removable storage medium shall be punished with imprisonment of either for a term which may extend to one year or	**3. Unauthorised access to information system or data.-** Whoever intentionally gains unauthorised access to any information system or data shall be punished with imprisonment for a term which may extend to three months or with fine up to fifty thousand rupees or with both.
56. Unlawful Intervention with Program or Data.- Whoever unlawfully damage or cause to be damaged an electronic system or network, data, electronic database or other program residing in such electronic system or network or disrupt or causes the disruption of an electronic system or network shall be punished with	**5. Interference with information system or data.-** Whoever intentionally interferes with or damages or causes to be interfered with or damaged any part or whole of an information system or data shall be punished with imprisonment which may extend to two years or with fine up to five hundred thousand rupees or with both.

imprisonment of either for a term which may extend to one year or with fine which may extend to three hundred thousand rupees or with both.	
57. Unauthorized Act with Information System.- Whoever unlawfully deny or cause the denial of access to a person authorized to obtain access to an electronic system or network by any means or charge the services availed of by a person to the account of another person by tampering with or manipulating an electronic system or network shall be punished with imprisonment of either for a term which may extend to three months or with fine which may extend to fifty thousand rupees or with both.	**8. Interference with critical infrastructure information system or data.-** Whoever intentionally interferes with or damages, or causes to be interfered with or damaged, any part or whole of a critical information system , or data , shall be punished with imprisonment which may extend to seven years or with fine up to ten million rupees or with both.
59. Cyber Extremism.- (1) Whoever commits or threatens to commit any of the offences,- (a) does any unauthorised act in relation to an information system; (b) at the time when he does the act he knows that it is unauthorised; and (c) acts with intent— (i) to destroy, damage, delete, erase, deteriorate, generate, modify or alter any program or data; (ii) to render any program or data inaccessible, meaningless, useless or ineffective; (iii) to obstruct, interrupt or interfere with any program or data or any aspect or attribute related to the program or data; (iv) to obstruct, interrupt or interfere with any person in the use of any program or data or any aspect or attribute related to the program or data; (v) to deny, prevent, suppress or hinder access to any program or data to any person entitled to it;	**10. Cyber terrorism. –** Whoever commits or threatens to commit any of the offences under sections 6, 7, 8 or 9 of this Act, where the commission or threat is with the intent to:- (a) coerce, intimidate, overawe or create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or (b) advance religious, ethnic or sectarian discord, shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine up to fifty million rupees or with both.

(vi) to deny, prevent, suppress or hinder access to any program or data or any aspect or attribute related to the program or data or make it inaccessible; (vii) to impair the operation of any program or any aspect or attribute related to the program; (viii) to impair the reliability of any data or any aspect or attribute related to the data; (ix) to impair the security of any program or data or any aspect or attribute related to the program or data; or (x) to enable any of the things mentioned in paragraphs (i) to (ix) to be done; shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to seven hundred thousand rupees, or with both. (2) Whoever commits any offence under sub-section (1) by circumventing or infringing security measures with respect to any information system, program or data shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to seven hundred thousand rupees or with both. (3) Whoever commits any offence under sub-section (1) with respect to any Government controlled critical infrastructure information system, program or data that performs a critical public function shall be punished with imprisonment of either description for a term which may extend to ten years or with fine which may extend to ten million rupees or with both. (4) Whoever intentionally, whether temporarily or not,— (a) does any unauthorised act in relation to an information system; (b) at the time when he does the act he	

knows that it is unauthorised; and (c) acts with intent— (i) to seriously interfere, hinder, damage, prevent, suppress, deteriorate, impair or obstruct the functioning of an information system; (ii) to seriously interfere, hinder, damage, prevent, suppress, deteriorate, impair or obstruct communication between or with an information system; (iii) to seriously interfere with or hinder access to any information system; (iv) to seriously impair the operation of any information system; (v) to seriously impair the reliability of any information system; (vi) to seriously impair the security of any information system; or (vii) to enable any of the things mentioned in paragraphs (i) to (vi) to be done; shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to seven hundred thousand rupees or with both. (5) Whoever commits any offence under sub-section (1) by circumventing or infringing security measures with respect to any information system, program or data shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to seven hundred thousand rupees or with both. (6) Whoever commits any offence under sub-section (1) with respect to any Government controlled critical infrastructure information system, program or data that performs a critical public function shall be punished with imprisonment of either description for a term which may extend to ten years or	

with fine which may extend to ten million rupees or with both. (7) Whoever commits any offence under sub-section (1),- (a) with respect to any Government controlled or public information system, program or data that performs a public function; and (b) that causes serious damage, injury or disruption to a widely and publicly utilized network of information systems; shall be punished with imprisonment of either description for a term which may extend to ten years or with fine which may extend to ten million rupees or with both. (8) However any person use or threat is designed to coerce, intimidate, overawe or create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or in society or the use or threat is made for the purpose or motive of advancing a cause whether political, religious, sectarian or ethnic, with the intention of. (i) interfering with, disrupting or damaging a public utility service or a communications system used by the public at large; or (ii) seriously interfering with, seriously disrupting or seriously damaging a designated payment system which interconnects with multiple financial institutions; (iii) seriously interfering with, seriously disrupting or seriously damaging a mass transportation or mass traffic system; (iv) seriously interfering with, seriously disrupting or seriously damaging a critical infrastructure that is used to serve a public function for the public at large; (v) seriously interfering with, seriously	

disrupting or seriously damaging critical infrastructure in use by the armed forces, civil armed forces, security forces or law enforcement agencies; (vi) causes injury through the acts mentioned in paragraphs (a), (c), (d) and (e); (vii) enabling any of the things mentioned in sub-paragraphs (i) to (vi) to be done; shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both. (9) Whoever commits any offence under sub-section (1) of this section by circumventing or infringing security measures with respect to any information system, program or data shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both. (10) However The intention referred to in sub-section (1) need not relate to,— (a) any particular information system; (b) any particular program or data; or (c) a program or data of any particular kind. (d) In this section,— (i) a reference to doing an act includes a reference to causing an act to be done; (ii) “act” includes a series of acts; (iii) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily; (e) a reference to an act by a person includes acts done or to be done,- (i) by or through an automated mechanism and self-executing, adaptive or autonomous device, program or information system; (ii) against Government controlled	

information systems or public information systems in exercise of a public function; or (iii) against any information system.	
60. Sending offensive messages through communication services, etc.- (1) A person shall not knowingly or without lawful excuse or justification send by means of an electronic system or an electronic device-information that is grossly offensive or has a menacing character; (a) information which he or she knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such electronic system or an electronic device; or (b) electronic mail or an electronic message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages. (2) For the purpose of this section, the term “electronic mail” or “electronic message” means a message or information created or transmitted or received on an electronic system or electronic device including attachments in text, images, audio, video and any other electronic record which may be transmitted with the message. (3) A person who contravenes sub-section (1) commits an offence shall be punished with imprisonment of either description for a term which may extend to two years or with fine which may extend to one hundred thousand rupees or with both.	**21. Cyber stalking.-** **(**1) Whoever with the intent to coerce or intimidate or harass any person uses information system, information system network, the Internet, website, electronic mail, information or any other similar means of communication to:- (a) communicate obscene, vulgar, contemptuous, or indecent information; or (b) make any suggestion or proposal of an obscene nature; or (c) threaten to commit any illegal or immoral act; or (d) take a picture or photograph of any person and display or distribute without his consent or knowledge in a manner that harms a person; or (e) display or distribute information in a manner that substantially increases the risk of harm or violence to any person, commits the offence of cyber stalking. (2) Whoever commits the offence specified in sub-section (1) shall be punishable with imprisonment for a term which may extend to one year or with fine up to one million rupees, or with both: Provided that if the victim of the cyber stalking under sub-section (1) is a minor the punishment may extend to five years or with fine upto ten million rupees, or with both. (3) Any aggrieved person may apply to the Authority for issuance of appropriate orders for removal or destruction of, or blocking access to such information as referred to in sub-section (1) and the Authority upon receipt of such application may take such measures as deemed appropriate for removal or destruction of, or blocking access to, such information.

(4) Identity theft,- (a) a person shall not knowingly or without lawful excuse or justification make fraudulent or dishonest use of an electronic signature, password or other unique identifying feature of another person. (b) a person who contravenes sub-section (1) commits an offence shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to three hundred thousand rupees or with both.	
61. Electronic forgery.- (1) A person shall not knowingly or without lawful excuse or justification, interfere with data or an electronic system so that he, she, or another person uses the data or the electronic system to induce a person to accept it as genuine and by reason of so accepting it to do or not to do any act to his or her own or any other person's prejudice or injury. (2) A person who contravenes sub-section (1) commits an offence shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to five hundred thousand rupees or with both.	**11. Electronic forgery.-** (1) Whoever, interferes with or uses any information system, device or data, with the intent to cause damage or injury to the public or to any person, or to make any illegal claim or title or to cause any person to part with property or to enter into any express or implied contract, or with intent to commit fraud by any input, alteration, deletion, or suppression of data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not shall be punished with imprisonment of either description for a term which may extend to three years, or with fine up to two hundred and fifty thousand rupees or with both. (2) Whoever commits offence under sub-section (1) in relation to a critical infrastructure information system or data shall be punished with imprisonment for a term which may extend to seven years or with fine up to five million rupees or with both.
62. Electronic fraud.-	**12. Electronic fraud:-**

(1) A person shall not knowingly or without lawful excuse or justification gain, interfere with data or an electronic system,– (a) to induce another person to enter into a relationship; (b) with intent to deceive another person; or (c) with intent to defraud a person, where such an act is likely to cause damage or harm to that person or any other person. (2) A person who contravenes sub-section (1) commits an offence shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to five hundred thousand rupees or with both.	Whoever with the intent for wrongful gain interferes with or uses any information system, device or data or induces any person to enter into a relationship or deceives any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment for a term which may extend to two years or with fine up to ten million rupees, or with both.
63. Violation of privacy.- (1) A person who, knowingly or without lawful excuse or justification, captures, publishes or transmits the image of a private area of a person without his or her consent, under circumstances violating the privacy of that person, commits an offence shall be punished with imprisonment of either description for a term which may extend to five years or with fine which may extend to five hundred thousand rupees or with both. (2) For the purposes of this section,– (a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons; (b) "capture" with respect to an image, means to videotape, photograph, film or record by any means; (c) "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;	**18. Offences against dignity of natural person-** (1) Whoever intentionally publicly exhibits or displays or transmits any false information, which is likely to harm or intimidate the reputation or privacy of a natural person shall be punished with imprisonment for a term which may extend to three years or with fine up to one million rupees or with both: Provided, nothing under this sub-section (1) shall apply to anything aired by a broadcast media or distribution service licensed under Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (XIII of 2002). (2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for passing of such orders for removal, destruction or blocking access to such information referred to in subsection (1) and the Authority on receipt of such application, may take such measures as deemed appropriate for securing, destroying, blocking access

(d) “publishes” means reproduction in the printed or electronic form and making it available for public; (e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that,– (i) he or she could disrobe in privacy, without being concerned that an image or his or her private area was being captured; or (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private **64. Child pornography.-** (1) For the purposes of this section a “child” means a person who is under the age of eighteen years. (2) A person shall not knowingly and without lawful justification or excuse,– (a) publish or transmit or cause to be published or transmitted material in an electronic form which depicts a child engaged in sexually explicit act or conduct; (b) create text or digital images, collect, seek, browse, download, advertise, promote, exchange or distribute material in an electronic form depicting a child in obscene or indecent or sexually explicit manner; (c) cultivate, entice or induce children to an online relationship with another child or an adult for a sexually explicit act or in a manner that may offend a reasonable adult on the electronic system; (d) facilitate the abuse of a child online; (e) record or own in an electronic form material which depicts the abuse of a child engaged in a sexually explicit act;	or preventing transmission of such information.

(f) procure and/or obtain child pornography through a computer system; or 45 (g) obtain access through information and communication technologies, to child pornography. (3) It is a defence to a charge of an offence under paragraphs (f) and (g) of sub-section (2) if the person can establish that the child pornography was for a bona fide law enforcement purpose. (4) A person who contravenes sub-section (2) commits an offence shall be punished with imprisonment of either description for a term which may extend to twelve years or with fine which may extend to five hundred thousand rupees or with both and in the event of second or subsequent shall be punished with imprisonment of either description for a term which may extend to twenty five years or with fine which may extend to ten million rupees or with both.. (5) Sub-section (2) does not apply to a book, pamphlet, paper, drawing, painting, representation or figure or writing in an electronic form,– (a) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or (b) which is kept or used for bona fide heritage or religious purposes.	
Chapter III Establishment of Investigation, Prosecution Agency and Special Court	**Chapter III Establishment of Investigation and Prosecution Agency and Procedural Powers for Investigation**

38. Establishment of investigation agencies and prosecution.- (1) The Federal Government shall establish new law enforcement agency as special Investigation Agency for the purposes of investigation and prosecution of offences under this Act. (2) Unless otherwise provided for under this Act the special investigation agency, the special investigating officer, prosecution and the court shall in all matters follow the procedure laid down in the Criminal Procedure Code (Act V of 1898) to the extent that it is not inconsistent with any provision of this Act: (3) All investigating officers appointed under this Act or exercising any power, privilege, right or provision under this Act shall at a minimum, hold a specialized qualification in digital forensics, information technology or computer science, in such terms as may be prescribed.	**26. Establishment of investigation agency.-** (1) The Federal Government may establish or designate a law enforcement agency as the investigation agency for the purposes of investigation of offences under this Act. (2) Unless otherwise provided for under this Act, the investigation agency, the authorised officer and the Court shall in all matters follow the procedure laid down in the Code to the extent that it is not inconsistent with any provision of this Act. (3) Notwithstanding provisions of any other law, the Federal Government shall make rules for appointment and promotion in the investigation agency including undertaking of specialized courses in digital forensics, information technology, computer science and other related matters for training of the officers and staff of the investigation agency.
39. Authority to investigate, warrant, arrest, search and seizer of material.- (1) No person whether a police officer investigation officer or otherwise other than an investigating officer of the special investigation agency shall investigate an offence with respect to, in connection with or under this Act. (2) No person other than a prosecutor assigned by the special investigating agency shall prosecute any offence with respect to, in connection with or under this Act. (3) No Court lower than the Special Court, in accordance with the provisions of this Act in particular section 45, shall conduct the trial, hearing of all proceedings in respect of, related to or in connection with an offence under this Act.	**27. Power to investigate.-** (1) Only an authorised officer of the investigation agency shall have the powers to investigate an offence under this Act: Provided that the Federal Government or the Provincial Government may, as the case may be, constitute one or more joint investigation teams comprising of the authorised officer of investigation agency and any other law enforcement agency for investigation of offence under this Act and any other law for the time being in force. **39. Offences to be compoundable and non-cognizable.-** (1) All offences under this Act, except the offences under section 10 and 19 of this

(4) No person, other than an investigating officer of the special investigation agency, shall exercise any power, including but not limited to arrest, access, search, seizure, preservation, production or real time collection or recording, under this Act, rules made thereunder or any other law, with respect to and in connection with any offence under this Act. (5) No investigating officer shall exercise any power of arrest, access, search, seizure, preservation, production, or real time collection other than a power provided for under this Act. (6) Notwithstanding any other law including sections 94 and 95 of CHAPTER VII Part B of the Code or any other provision of any law, and without prejudice to and subject at all times to sections 41, 42, 43 and 44 of this Act, no investigating officer shall conduct any inquiry or investigation or call for any information in connection with any offence under this Act without obtaining an order for the disclosure of such information from the Court and the Court shall only issue such order if the particulars of the investigation meet the qualification provided for under the relevant section of this Act to which the request for disclosure pertains. (7) Any investigating officer, when mentioning any section of this Act in any application or any document, including but not limited to any application for any warrant or disclosure under this Act or any report under sections 154, 155 or 173 or any other provision of the Code of Criminal Procedure or any other law with respect to any investigation, inquiry, arrest, access, search, seizure, preservation, production, or real time collection under this Act, shall not merely	Act , and abetment thereof, shall be non-cognizable, bailable and compoundable: Provided that offences under section 15 of this Act shall be cognizable by the investigation agency on a written complaint by the Authority. (2) Offences under section 10 and19 of this Act and abetment thereof shall be non-bailable, non-compoundable and cognizable by the investigation agency. **36. Real-time collection and recording of information.-** (1) If a Court is satisfied on the basis of information furnished by an authorised officer that there are reasonable grounds to believe that the content of any information is reasonably required for the purposes of a specific criminal investigation, the Court may order, with respect to information held by or passing through a service provider, to a designated agency as notified under the Investigation for Fair Trial Act, 2013 (I of 2013) or any other law for the time being in force having capability to collect real time information, to collect or record such information in real-time in coordination with the investigation agency for provision in the prescribed manner: Provided that such real-time collection or recording shall not be ordered for a period beyond what is absolutely necessary and in any event for not more than seven days. (2) Notwithstanding anything contained in any law to the contrary the information so collected under subsection (1) shall be admissible in evidence. (3) The period of real-time collection or recording may be extended beyond seven days if, on an application, the

mention the section but shall also specify the sub-section, paragraph and sub-paragraph to identify exactly which offence is being referred to.	Court authorises an extension for a further specified period. (4) The Court may also require the designated agency to keep confidential the fact of the execution of any power provided for in this section and any information relating to it. (5) The application under sub-sections (1) and (2) shall in addition to substantive grounds and reasons also- (a) explain why it is believed the data sought will be available with the person in control of an information system; (b) identify and explain with specificity the type of information likely to be found on such information system; (c) identify and explain with specificity the identified offence made out under this Act in respect of which the warrant is sought; (d) if authority to seek real-time collection or recording on more than one occasion is needed, explain why, and how many further disclosures are needed to achieve the purpose for which the warrant is to be issued; (e) what measures shall be taken to prepare and ensure that the real-time collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information of any person not part of the investigation; (f) why the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and (g) why to achieve the purpose for which the warrant is being applied, real time collection or recording by the person in control of the information system is necessary

40. Expedited Preservation of data.- (1) If an investigating officer is satisfied that- (a) traffic data or content data stored in any information system or by means of an information system, is reasonably required for the purposes of a criminal investigation; and (b) there is a risk or vulnerability that the traffic data or content data may be modified, lost, destroyed or rendered inaccessible, the investigating officer may, by written notice given to a person in control of the information system, require the person to ensure that the data specified in the notice be preserved and the integrity thereof is maintained for a period not exceeding seven days as specified in the notice. (2) The period of preservation and maintenance of integrity may be extended beyond seven days if, on an application by the investigating officer, the Court authorizes an extension for a further specified period of time, upon being satisfied that reasonable cause for such extension exists. (3) The person in control of the information system shall only be responsible to preserve the data specified- (a) for the period of the preservation and maintenance of integrity notice or for any extension thereof permitted by the Court; (b) to the extent that such preservation and maintenance of integrity will not be administratively or financially burdensome; and (c) where it is technically and practically reasonable to preserve and maintain the integrity such data.	**28. Expedited preservation and acquisition of data.-** (1) If an authorised officer is satisfied that- (a) data stored in any information system or by means of an information system, is reasonably required for the purposes of a criminal investigation; and (b) there is a risk or vulnerability that the data may be modified, lost, destroyed or rendered inaccessible, the authorised officer may, by written notice given to a person in control of the information system, require that person to provide that data or to ensure that the data specified in the notice be preserved and the integrity thereof is maintained for a period not exceeding ninety days as specified in the notice: Provided that the authorized officer shall immediately but not later than twenty four hours bring to the notice of the Court, the fact of acquisition of such data and the court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case including issuance of warrants for retention of such data or otherwise. (2) The period provided in sub-section (1) for preservation of data may be extended by the Court if so deemed necessary upon receipt of an application from the authorised officer in this behalf.

41. Warrant for search and seizure.- (1) Upon an application on oath by an investigating officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that there may be in a specified place an information system, program, data, device or storage medium of a specified kind that- (a) is reasonably required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence made out under this Act; or (b) has been acquired by a person as a result of the commission of an offence, the Court may after recording reasons, issue a warrant which shall authorise an investigation officer, with such assistance as may be necessary, in the presence of a Magistrate, to enter only the specified place and to search only the specified information system, program, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure only the specified data or specified program, device or storage medium relevant to the offence identified in the application, but without causing any of the results identified in any event without prejudicing the integrity and security of any data or program available in or through the specified information system, program or generally present or available at the specified place: Provided that the Magistrate for the purposes of this Chapter shall not include any person who is employed or performs any function on behalf of the special investigating agency:	**30. Warrant for search or seizure.-** (1) Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that there may be in a specified place an information system, data, device or other articles that- (a) may reasonably be required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence made out under this Act; or (b) has been acquired by a person as a result of the commission of an offence, the Court may issue a warrant which shall authorise an officer of the investigation agency, with such assistance as may be necessary, to enter the specified place and to search the premises and any information system, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure any information system, data or other articles relevant to the offence identified in the application. (2) In circumstances involving an offence under section 10 of this Act, under which a warrant may be issued, but cannot be obtained without affording opportunity of destruction, alteration or loss of data, information system, device or any other article required for investigation, the authorized officer who shall as far as practicable be a Gazetted officer of the investigation agency enter the specified place and search the premises and any information system, data, device or article relevant to the offence and access, seize or similarly secure any information system, data or other articles relevant to the offence: Provided that the authorized

Provided further that the requirement of the presence of a Magistrate under paragraph (b) of sub-section (1) and paragraph (h) of sub-section (2) shall come into effect twelve months from the coming into force of this Act. (2) The application under sub-section (1) shall in addition to substantive grounds and reasons also,- 26 (a) explain why it is believed the material sought will be found on the premises to be searched; (b) why the purpose of a search may be frustrated or seriously prejudiced unless an investigating officer arriving at the premises can secure immediate entry to them; (c) identify and explain with specificity the type of evidence suspected will be found on the premises; (d) identify and explain with specificity the relevant program or data that is sought and reasonably suspected to be available from each individual information system, device or storage medium; (e) identify and explain with specificity the relevant individual information systems, devices or storage mediums expected to be searched or seized and reasonably suspected to contain the relevant program or data or any evidence; (f) what measures shall be taken to prepare and ensure that the search and seizure is carried out through technical means such as mirroring or copying of relevant data and not through physical custody of information systems or devices; Provided that this shall not prejudice the powers defined in sub-section (4) of section 39;	officer shall immediately but not later than twenty four hours bring to the notice of the Court, the fact of such search or seizure and the court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case.

(g) describe and identify the persons to be authorised to accompany the officer executing the warrant and the reasons that necessitate their presence; and (h) seek the Court to identify the Magistrate who will be accompanying the officer during execution of the warrant. (3) No Court shall issue any warrant to enter and search any specific premises, any specific information system or any specific program or any specific data or any specific device or any specific storage medium unless satisfied that consequent upon the particulars of the offence referred to in the application, there are reasonable grounds for believing that it is necessary to search any specific premises occupied, any specific information system or any specific program or any specific data or any specific device or any specific storage medium controlled by the person identified in the application in order to find the material sought. 27 (4) Any person who obstructs the lawful exercise of the powers under sub-section (1) or sub-section (2) or misuses the powers granted under this section shall be liable to punishment with imprisonment of either description for a term which may extend to six month, or with fine not exceeding fifty thousand rupees, or with both.	
43. Powers of an investigating officer.- (1) Subject to obtaining a search warrant under section 39 an investigation officer shall be entitled to only the information system, program and data specified in the warrant to-	**32. Powers of an authorized officer.-** (1) Subject to provisions of this Act, an authorised officer shall have the powers to - (a) have access to and inspect the operation of any specified information system;

(a) have access to and inspect the operation of any specified information system; (b) use or cause to be used any such specified information system to search any specified data contained in or available to such information system; (c) obtain and copy that data, use equipment to make copies and obtain an intelligible output from an information system; (d) have access to or demand any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such information system into readable and comprehensible format or plain version; (e) require any person by whom or on whose behalf, the investigating officer has reasonable cause to believe, any information system has been used to grant access to any data within any information system within the control of such person; (f) require any person having charge of or otherwise concerned with the operation of such information system to provide him reasonable technical and other assistance as the investigating officer may require for the purposes of paragraphs (a), (b) and (c); and (g) require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence: Provided that this power shall not empower an investigating officer to compel a suspect or an accused to provide decryption information, or to	(b) use or cause to be used any specified information system to search any specified data contained in or available to such system; (c) obtain and copy only relevant data, use equipment to make copies and obtain an intelligible output from an information system; (d) have access to or demand any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such information system into readable and comprehensible format or plain version; (e) require any person by whom or on whose behalf, the authorised officer has reasonable cause to believe, any information system has been used to grant access to any data within an information system within the control of such person; (f) require any person having charge of or otherwise concerned with the operation of any information system to provide him reasonable technical and other assistance as the authorised officer may require for investigation of an offence under this Act; and (g) require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence: Explanation.- Decryption information means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable form and from ciphered data to intelligible data.

incriminate himself or provide or procure information or evidence or be a witness against himself. Explanation.-Decryption information means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable form and from cipher text to its plain text. (2) In exercise of the power of search and seizure of any information system, program or data the investigating officer shall- (a) at all times act with proportionality; (b) take all precautions to maintain integrity of the information system, program and data subject of the search or seizure in respect of which a warrant has been issued; (c) not disrupt or interfere with the integrity or running and operation of any information system, program or data that is not the subject of the offences identified in the application for which a warrant for search or seizure has been issued; (d) avoid disruption to the continued legitimate business operations and the premises subject of the search or seizure; and (e) avoid disruption to any information system, program or data not connected with the information system that is not the subject of the offences identified in the application for which a warrant has been issued or is not necessary for the investigation of the specified offence in respect of which a warrant has been issued. (3) When seizing or similarly securing any data, the investigating officer shall make all efforts to use technical measures to copy or replicate the data,	(2) In exercise of the power of search and seizure of any information system, program or data the authorized officer at all times shall- (a) act with proportionality; (b) take all precautions to maintain integrity of the information system and data in respect of which a warrant for search or seizure has been issued; (c) not disrupt or interfere with the integrity or running and operation of any information system or data that is not the subject of the offences identified in the application for which a warrant for search or seizure has been issued; (d) avoid disruption to the continued legitimate business operations and the premises subjected to search or seizure under this Act; and (e) avoid disruption to any information system, program or data not connected with the information system that is not the subject of the offences identified in the application for which a warrant has been issued or is not necessary for the investigation of the specified offence in respect of which a warrant has been issued (3) When seizing or securing any information system or data, the authroised officer shall make all efforts to use technical measures while maintaining its integrity and chain of custody and shall only seize an information system, data, device or articles, in part or in whole, as a last resort, for sufficient reasons that do not make it possible under the circumstances to use such technical measures or where use of such technical measures by themselves would not be sufficient to maintain the integrity and chain of custody of the data being seized.

whilst maintaining its integrity and chain of custody and shall only seize any information system, device or storage medium physically, in whole or in part, as a last resort, for sufficient reasons that do not make it possible under the circumstances to use such technical measures or where use of such technical measures by themselves would not be sufficient to maintain the integrity and chain of custody of the data being seized: Provided that where a physical seizure occurs, the investigating officer shall submit forthwith and in any event no later than twenty four hours a report detailing sufficient reasons for such seizure before the Court.	
45. Establishment of Special Courts etc.- (1) The Government may establish as many Special Courts under this Act however special court may be established at district level of all provinces of Pakistan. (2) The Government, in consultation with the Chief Justice of the concerned High Court, may appoint any person as judge of the Special Court constituted under this Act who is or has been a Sessions Judge in any province of Pakistan or has been an Advocate of the High Court for a period of not less than ten years. (3) Only a Court where the presiding judge has successfully completed training conducted by the Federal Judicial Academy with respect to all aspects of this Act including cyber forensics, electronic transactions and data protection shall be competent to hear any matter arising out of or in connection with	**40. Cognizance and trial of offences.-** (1) The Federal Government, in consultation with the Chief Justice of respective High Court, shall designate Presiding Officers of the Courts to try offences under this Act at such places as deemed necessary. (2) The Federal Government shall, in consultation with the Chief Justice of respective High Court, arrange for special training to be conducted by an entity notified by the Federal Government for training on computer sciences, cyber forensics, electronic transactions and data protection. (3) Prosecution and trial of an offence under this Act committed by a minor shall be conducted under the Juvenile Justice System Ordinance, 2000. (4) To the extent not inconsistent with this Act, the procedure laid down under the Code of Criminal Procedure 1898 (V of 1898) and the Qanoon-e-Shahadat Order

this Act. (4) A judge Special Court shall have all the powers of a Sessions Court as provided under the Code.	1984 (X of 1984) shall be followed.
46. Appeal.- (1) An appeal against the final judgment of a Special Court shall lie to the High Court. (2) Copies of the judgments of a Special Court shall be supplied to the accused and public prosecutor on the day the judgment is pronounced. (3) Any aggrieved person or the Government may file an appeal against the final judgment of a Special Court within a period of thirty days from the pronouncement of judgment.	**43. Appeal.-** An appeal against the final judgment of a Court shall lie within thirty days from the date of provision of its certified copy free of cost.
52. Limitation of liability of intermediaries and service providers.- (1) No intermediary or service provider shall be subject to any civil or criminal liability, unless it is finally established that the intermediary or service provider had actual notice, specific actual knowledge, willful and malicious intent and motive to proactively and positively participate, and not merely through omission or failure to act, and thereby facilitated, aided or abetted the use by any person of any information system, service, application, online platform or telecommunication system maintained, controlled or managed by an intermediary or service provider in connection with a contravention of this Act, rules made thereunder or any other law:Provided that the burden to prove that an intermediary or service provider had notice, specific actual knowledge, willful and malicious intent and motive to proactively and positively participate in any act that gave	**35. Limitation of liability of service providers.-** (1) No service provider shall be subject to any civil or criminal liability, unless it is established that the service provider had specific actual knowledge and willful intent to proactively and positively participate, and not merely through omission or failure to act, and thereby facilitated, aided or abetted the use by any person of any information system, service, application, online platform or telecommunication system maintained, controlled or managed by the service provider in connection with a contravention of this Act or rules made thereunder or any other law for the time being in force: Provided that the burden to prove that a service provider had specific actual knowledge, and willful intent to proactively and positively participate in any act that gave rise to any civil or criminal liability shall be upon the person alleging such facts and no interim

rise to any civil or criminal liability shall be upon the person alleging such facts and no interim or final orders, directions shall be issued with respect to any intermediary or service provider unless such facts have so been finally proved: Provided further that such allegation and its proof shall clearly identify with specificity the content, material or other aspect with respect to which civil or criminal liability is claimed including but not limited to unique identifiers such as the Account Identification (Account ID), Uniform Resource Locator (URL) Top Level Domain (TLD) Internet Protocol Addresses (IP Addresses) or other unique identifier and clearly state the statutory provision and basis of the claim. (2) No intermediary or service provider shall under any circumstance be liable under this Act, rules made thereunder or any other law for maintaining and making available the provision of their service. (3) No intermediary or service provider shall be subject to any civil or criminal liability as a result of informing a subscriber, user or end-users affected by any claim, notice or exercise of any power under this Act, rules made thereunder or any other law: Provided that the intermediary or service provider present and established in terms equivalent to the requirements of the Companies Ordinance 1984 within the territorial jurisdiction of Pakistan, for a period not exceeding fourteen days, shall keep confidential and not disclose the existence of any investigation or exercise of any power under this Act when a notice to this effect is served upon them by an investigating officer, which period of confidentiality may be extended beyond fourteen days if, on an application	or final orders, or directions shall be issued with respect to a service provider by any investigation agency or Court unless such facts have so been proved and determined: Provided further that such allegation and its proof shall clearly identify with specificity the content, material or other aspect with respect to which civil or criminal liability is claimed including but not limited to unique identifiers such as the Account Identification (Account ID), Uniform Resource Locator (URL), Top Level Domain (TLD), Internet Protocol Addresses (IP Addresses), or other unique identifier and clearly state the statutory provision and basis of the claim. (2) No service provider shall under any circumstance be liable under this Act, rules made thereunder or any other law for maintaining and making available the provision of their service in good faith. (3) No service provider shall be subject to any civil or criminal liability as a result of informing a subscriber, user or end-users affected by any claim, notice or exercise of any power under this Act, rules made thereunder or any other law: Provided that the service provider, for a period not exceeding fourteen days, shall keep confidential and not disclose the existence of any investigation or exercise of any power under this Act when a notice to this effect is served upon it by an authorised officer, which period of confidentiality may be extended beyond fourteen days if, on an application by the authorised officer, the Court authorises an extension for a further specified period upon being satisfied that reasonable cause for such extension exists.

by the investigating officer, the Court authorizes an extension for a further specified period of time, upon being satisfied that reasonable cause for such extension exists. (4) No intermediary or service provider shall be liable under this Act, rules made thereunder or any other law for the disclosure of any data or other information that the service provider discloses only to the extent of and under sub-section (3) and sections 40, 41, 42 and 43. (5) No intermediary or service provider shall be under any obligation to proactively monitor, make inquiries about material or content hosted, cached, routed, relayed, conduit, transmitted or made available by such intermediary or service provider.	(4) No service provider shall be liable under this Act, rules made thereunder or any other law for the disclosure
Chapter V Miscellaneous	**Chapter VII Miscellaneous**
66. Application of Electronic Transactions Ordinance, 2002.- (1) Without prejudice to the application of the Electronic Transactions Ordinance, 2002 or any of its provisions, including sub-section (2) of section 16 or paragraph (f) of sub-section (1) of section 2 to the Electronic Transactions Ordinance, 2002 and any other law, the Federal Government may prescribe rules for communication, filing, submission or processing of any pleadings, evidence or documents by any person, including but not limited by or before the Court or by the investigating officer, the prosecutor, complainant or accused, with respect to any application or exercise of any power or provision under this law through	**49. Amendment of Electronic Transactions Ordinance, 2002 (LI of 2002) and pending proceedings:-** (1) Sections 36 and 37 of the Electronic Transactions Ordinance, 2002 (LI of 2002) are omitted. (2) Any action taken by or with the approval of the authority or proceedings pending under the provisions of the Electronic Transactions Ordinance, 2002 (LI of 2002) repealed by sub-section (1), shall continue and be so deemed to have been taken or initiated under this Act.

electronic means or in electronic form. (2) When prescribing rules for the application under sub-section (1), the Federal Government shall have due regard to the availability, accessibility, security, authenticity and integrity of the electronic form or electronic means by which the enabling powers under sub-section (1) may be exercised by the Court, prosecutor, investigation agency or any other person. Explanation:- The Federal Government may, where it is appropriate in terms of the availability, accessibility and security, prescribe rules for the communicating, filing, submissions and processing of applications, pleadings and evidence and other documents in electronic form before the Court or by the prosecution, the investigation agency, complainant, accused or any other person. The use of these means would include instances such as electronic applications for any warrants; the supply of statements and documents to the accused; supply of evidence recorded; applying for a copy of seized data and other provisions under this law. However, the Federal Government shall ensure that such rules shall provide for the security, integrity and authenticity at all times of such means of communication, filing, submission and processing and only enable these means at locations where appropriate under the circumstances.	
68. Savings of Intelligence Services powers.- (1) Offences, powers and procedures provided under this Act are not related to and have no application upon the activities, powers or functions of intelligence agencies or services and are without prejudice to the operation of or	**50. Savings of powers:** Nothing in this Act shall affect, limit or prejudice the duly authorized and lawful powers and functions of the institutions controlled by the Federal and Provincial governments performed in good faith.

powers exercised under- (a) section 54 of the Pakistan Telecommunication (Re-organization) Act, 1996; (b) the Army Act, 1952; (c) the Air Force Act, 1953; (d) the Navy Ordinance, 1961; (e) the purview of the Intelligence Bureau; (f) the investigation agency or intelligence service notified by the Federal Government under section 38 of this Act; and (g) any other intelligence agency or service that does not itself undertake the investigation or prosecution of any criminal offence.	
69. Act to override other laws.- The provisions of this Act shall have effect notwithstanding anything to the contrary contained in any other law and shall survive any amendment of any other law unless specifically amended or repealed.	**46. Relation of the Act with other laws.-** (1) The provisions of this Act shall have effect not in derogation of the Pakistan Penal Code, 1860 (XLV of 1860), the Code of Criminal Procedure, 1898 (V of 1898) and the Qanoon-e-Shahadat Order, 1984 (X of 1984), Protection of Pakistan Act, 2014 (X of 2014) and Investigation for Fair Trial Act, 2013 (I of 2013). (2) Subject to sub-section (1), the provisions of this Act shall have effect notwithstanding anything to the contrary contained in any other law on the subject for the time being in force.
70. Power to amend Schedule.- The Federal Government may, by notification in the official Gazette, amend the Schedule so as add any entry thereto but not omit any entry therein.	**47. Power to make rules.-** (1) The Federal Government may, by notification in the official Gazette, make rules for carrying out purposes of this Act. (2) Without prejudice to the generality, of the foregoing powers, such rules may specify:- (a) qualifications and trainings of the officers and staff of the investigation agency and prosecutors; (b) powers,

	functions and responsibilities of the investigation agency, its officers and prosecutors; (c) standard operating procedures of the investigation and prosecution agency; (d) mode and manner in which record of investigation under this Act may be maintained; **48. Removal of difficulties.-** If any difficulty arises in giving effect to the provisions of this Act, the Federal Government may, within two years of commencement of this Act by order published in the official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary for removing the difficulty.