INTRODUCED ON 14-04-2014

[AS INTRODUCED IN THE SENATE]

A

BILL

to provide for the establishment of a National Cyber Security Council

WHEREAS it is expedient to establish a high level policy making and over seeing Council, to provide enabling environment, conduct research and analysis, enhance capacity, develop policy, and strategies, advise various branches of the Government, Academia, and Information Security professionals; facilitate the Non State Actors and private sector in continually improving the state of readiness to ensure Cyber Security of Pakistan; cultivate awareness, responsibility and help build capacity as individuals, organizations and companies to take responsibility for securing own part of cyber space; and also educate that the digital regime stretches around the globe and does not recognize any legal or geographical boundary. The standards of precautions, preventions and preparations, therefore, need to match the globally acceptable parameters.

1. Short title, extent, application and commencement.-(1) This Act may be called the National Cyber Security Council Act, 2014.

(2) It extends to the whole of Pakistan.

(3) It shall come into force at once.

2. Definitions.- (1) In this Act, unless there is anything repugnant in the subject or context,-

(a) **"Act"** means the National Cyber Security Council Act, 2014;

(b) **"Advisory Group"** means an Advisory Group as may be constituted under section 10;

(c) **"CERT"** means Cyber Emergency Response Team;

(d) **"Chairman"** means the Chairman of the National Cyber Security Council;

(e) **"Council"** means the National Cyber Security Council;

(f) **"Cyber Security"** means the definition as may be developed by the National Cyber Security Council from time to time, given the fast moving dynamism in the subject fields and the need to respond with equivalent enhanced capacity, speed and effectiveness, to the emerging threats to Cyber Security, provided that at all times the definition so developed shall not be over reaching, arbitrary, inconsistent, unique or conflicting in any manner with the globally accepted international best practices, adopted by the leading developed nation states;

(g) **"Entity"** includes an individual, appropriate authority, trust, waqf, association, statutory body, firm, company including joint venture or consortium, or any other entity, whether registered or not;

(h) **"Government"** means the Federal, Provincial or local Government, or any local authority, statutory body, corporation, financial institution, bank, authority undertaking or any other organization or entity that that is controlled, managed or operated in any manner and to any extent by or under the authority of the Federal Government, or the Provincial Government concerned;

(i) **"ISPAK"** means the Internet Service Providers Association of Pakistan, or its successor by whatever name called;

(j) **"PASHA"** means the Pakistan Software Houses Association, or its successor by whatever name called;

(k) **"PISA"** means the Pakistan Information Security Association, or its successor by whatever name called;

(l) **"prescribed"** means prescribed by the Rules;

(m) **"Rules"** means rules made under this Act; and

(n) **"Schedule"** means the Schedule to this Act;

THE NATIONAL CYBER SECURITY COUNCIL

3. Establishment of National Cyber Security Council.–(1) Within sixty days of the enactment of this Act, the Senate Standing Committee on Defence shall constitute the National Cyber Security Council.

(2) No act of the Council shall be invalid by reason only of the existence of any vacancy among its members or any defect in its constitution discovered after such act or proceeding of the Council:

Provided that as soon as such defect has been discovered, the member shall not exercise the functions or powers of his membership until the defect has been rectified.

(3) The Council shall meet at least once in each quarter of a year.

(4) The Council may from time to time delegate one or more of its functions and powers to one or more of its members, however, under no circumstance shall be further delegated.

(5) Decisions of the Council shall be taken by a majority of the members.

(6) Save as provided herein, the terms and conditions of service of the members of the Council shall be such as may be prescribed.

4. Members. (1) The Council shall comprise following members, with 21 members from the Federal Government, including the Chairman, who shall be the Chairman, Senate Standing Committee on Defence and rest of the members from the private sector and Information Security Professionals.

(a) The members from the Federal Government shall be the following or their designate to act on their behalf:-

(i)	Chairman, Senate's Standing Committee on Defence;	Chairman
(ii)	Attorney General for Pakistan;	Member
(iii)	Governor State Bank of Pakistan;	Member
(iv)	Auditor General of Pakistan;	Member
(v)	Secretary, Ministry of Defence;	Member
(vi)	Secretary, Finance Division;	Member
(vii)	Secretary, Planning Division;	Member
(viii)	Secretary, Ministry of Interior;	Member
(ix)	Secretary, Ministry of Law;	Member
(x)	Secretary, Cabinet Division;	Member
(xi)	Secretary, Senate Secretariat;	Member
(xii)	Secretary, Narcotics Control Division;	Member
(xiii)	Chairman, National Disaster Management Authority(NDMA);	Member
(xiv)	Rector, National University of Science and Technology (NUST);	Member
(xv)	Rector, COMSATS Institute of Information Technology;	Member
(xvi)	Director General, Federal Investigation Agency(FIA);	Member
(xvii)	Chairman, National Database and Registration Authority (NADRA);	Member
(xviii)	Director General, Department of Communication Security;	Member
(xix)	National Coordinator, National Counter Terrorism Authority (NACTA);	Member
(xx)	Project Director, National Forensic Science Agency (NFSA);	Member
(xxi)	Secretary, Ministry of Information Technology;	Member/Secretary

(b) The members from the private sector shall, interalia, comprise of the following:-

(i)	two Technical Experts to be designated by appropriate fora;	Members
(ii)	two Legal Experts to be designated by Attorney General for Pakistan;	Members
(iii)	Researcher/Academia to be nominated by appropriate fora;	Member
(iv)	one member to be nominated by the ISPAK;	Member
(v)	one member to be nominated by the PASHA;	Member
(vi)	one member to be nominated by the PISA;	Member
(vii)	one member to be nominated by the Computer Society of Pakistan;	Member
(viii)	two representatives of large business to be designated by the Federation of Chambers of Commerce and Industry of Pakistan;	Members
(ix)	one representative of small business to be designated by the Federation of Chambers of Commerce and Industry of Pakistan;	Member
(x)	two Chartered Accountants with relevant professional experience to be designated by competent and appropriate fora; and	Members
(xi)	two Digital Forensic Investigators to be designated by appropriate and competent for a.	Members

Provided that the members from the private sector, shall have at least seven years of practical experience, domestically and/or internationally, in Cyber Security.

(2) PASHA, ISPAK and PISA etc., may with the approval of the Chairman of the Council, appoint, replace, appoint alternates and appoint subsequent members from the private sector.

(3) The private sector/academia members of the Council shall be appointed for a term of two years and shall be eligible for reappointment.

5. Functions and powers of the Council.- (1) The Council shall, interalia, perform such functions as are specified in this Act or may be prescribed from time to time by the Council.

(2) Without prejudice to the generality of the foregoing sub-section, the Council shall,-

(a) develop policy, render advice, conduct research and establish start up initiatives;

(b) establish a National Cyber Security strategy which may be updated from time to time, as and when deemed appropriate, but not later than every three years;

(c) establish an International Cyber Security strategy which may be updated from time to time, as and when deemed appropriate but not later than every three years;

(d) undertake initiatives as provided for under section 6;

(e) develop and draft policy, guidelines and governance models related to ever emerging Cyber Security threats;

(f) advise and make recommendations to the Senate and the National Assembly, Judiciary and all Ministries, Departments and branches of Government on policy and legislation with respect to Cyber Security;

(g) monitor legislation and provide advice and recommendations with the objective of ensuring that legislation reflects international best practices with respect to Cyber Security;

(h) advise and make recommendations to Government departments on mechanisms to implement policies related to Cyber Security and monitor and have performance audit conducted thereof;

(i) make recommendations to the Government for adoption either through policies and regulatory means of standardization, harmonization and accreditation with regards to critical information infrastructure;

(j) coordinate and consult with all representative state and non-state actors on implementation of policies, initiatives and legislation on Cyber Security;

(k) facilitate communications between the Government and private sector entities, Academia, Cyber Security experts through multi-stakeholder meetings held with such frequency as determined necessary by the Council;

(l) establish the Advisory Groups as provided by section 10 to provide non binding input to the National Cyber Security Council on strategic plans as and when called upon to do so from time to time;

(m) in particular advise, assist, collaborate and coordinate with National Security apparatus of the State of Pakistan for continually improving the state of Cyber Security with respect to all aspects and interests of the State;

(n) coordinate, collaborate and conduct exchanges with international bodies, fora and entities, interalia, in connection with the functions and powers herein;

(o) cause research and development to be conducted with respect to Kaleidoscopic Cyber Security threats, developments, best practices and international laws and obligations;

(p) promote general awareness with respect to Cyber Security awareness, particularly the in-house role and responsibility of individuals, corporate entities and organizations ;

(q) develop a ten year and twenty year vision with regards to Cyber Security;

(r) legislate and update such Rules for the internal administration and operations of the Council, its personnel and Advisory Groups, as it may consider appropriate for carrying out the purposes of this Act;

(s) Inclusively, collaborate with the corporate entities, private sector, cyber security academia, professionals, civil society and community to achieve the objectives;

(t) the Council may delegate the functions and powers in paragraphs (o) to (q) to any one or more of the Advisory Groups, as it deems appropriate.

6. Initiatives.- (1) The Council shall have the function of and powers to devise strategic plans and develop and establish start up initiatives pertinent to Cyber Security in accordance with the respective strategic plan.

(2) The initial initiatives shall, interalia, include those listed in Schedule-I. The Contents of Schedule-I are only illustrative and not exhaustive. Further initiatives shall be added there as and when concurred.

7. Oversight.- The Senate Standing Committee on Defence shall oversee the administration and functions of the Council.

8. Lean Personnel and unconventional management model, consisting of appropriately qualified and experienced, professionals in Cyber Security discipline.- The Council shall requisition services of the following personnel, appropriately qualified and experienced in cyber security discipline from the Establishment Division for posting on transfer:

(a)	Secretary (BPS-20-21)	01
(b)	Computer Personnel (BPS-17, 18, 19 & 20)	05

9. Functions of the Secretary and his team.- (1) The Secretary shall perform the functions of a Chief Executive Officer with respect to the Council and such functions as are specified in this Act or may be prescribed by the Council, from time to time.

(2) Without prejudice to the generality of the foregoing sub-section, the Secretary shall,-

(a) within one year after the date of enactment of this Act, complete a comprehensive review of the Federal statutory and legal framework applicable to the cyber-related threats and feasible responses in Pakistan;

(b) upon completion of the review, submit a report to the Council containing the findings, conclusions and recommendations.

10. Advisory Groups.- (1) The Council shall constitute the following Advisory Groups which would be encouraged to render issue based and policy oriented advice and recommendations to the Council from time to time:

(a) **Operational Advisory Group**, interalia, shall include the following members: the Pakistan Telecommunication Authority, the Federal Investigation Agency, the Intelligence Bureau, the Inter Services Intelligence, the Military Intelligence, the Inspector General of Sindh, the Inspector General of Punjab, the Inspector General of Balochistan, the Inspector General of Khyber Pakhtunkhwa, the Inspector General of Islamabad Capital Territory, Inspector General of AJK, Inspector General of Gilgit Baltistan, Inspector Generals, Special Branches of all Provinces, Chairman, FBR, Chairman, NAB, Accountant General Pakistan Revenues, Anti Narcotics Force, Competition Commission of Pakistan, Controller General of Accounts, Directorate General Immigration & Passport, Electronic Government Directorate, Frequency Allocation Board, Intellectual Property Organization, Law & Justice Commission of Pakistan, Military Accountant General, National Crises Management Cell, National Highways and Motorways Police, National Institute of Electronics, National Radio Telecommunication Corporation, National Telecommunication Corporation, Pakistan Atomic Energy Commission(PAEC), Pakistan Computer Bureau, Securities & Exchange Commission of Pakistan, Special Communication Organization (SCO), Pakistan Software Export Board, Telecommunication and Cellular Companies, Internet Service Providers, hardware/software providers may, if they so choose, participate in the meetings by special invitation as well;

(b) **Technical Advisory Group**, interalia, shall include the following members: members from science, technology and engineering universities, research institutes, technical laboratories, white collar crime detectives/investigators cryptologists, cryptographers, encryption experts, cyber security professionals, white-hat hackers, mathematicians, other scientific and technical experts, researchers and academics, Allama Iqbal Open University, SDIP, Jinnah Institute, Institute of Strategic Studies, International Islamic University, National Defence University, National Police Academy, Pakistan Council for Science & Technology, Pakistan Council of Scientific & Industrial Research, Pakistan Scientific and Technological Information Centre, chief security officers, chief information officers and chief information security officers, chief information officers and chief information security officers of financial institutions;

(c) **Policy Advisory Group**, interalia, shall include the following members: policy institutes, think tanks, policy experts and consultants, legal experts, Digital Forensic, corporate & financial lawyers, High Courts/Supreme Court Bar Councils, Digital Forensic Auditors, hand writing, thumb impressions experts, questioned documents' analysts, anti money laundering professionals and consultants, strategists, defence experts, war study experts, National security experts and law enforcement experts;

(d) **Industry Advisory Group**, interalia, shall include the following members: : industry associations or representative bodies, management consultants, industry chief executive officers, particularly chief executives of financial institutions, the Federation of Pakistan Chamber of Commerce and Industry, the Karachi Chamber of Commerce and Industry, the Lahore Chamber of Commerce and Industry, the Islamabad Chamber of Commerce and Industry, the Over Seas Investors Chamber Of Commerce and Industry and the International Chamber of Commerce;

Provided that the advice rendered by the Advisory Groups shall not be construed in any manner to be binding or requiring any implementation or consultation of any form and shall be advice rendered which may or may not be followed at the sole and absolute discretion of the Council.

(2) Members of the Council may, if they so choose, be members of any of the Advisory Groups.

NATIONAL CYBER SECURITY COUNCIL FUND

11. National Cyber Security Council Fund.- (1) The Council shall, interalia, endeavor in the realms of creating awareness, building intellectual property and generating digital deterrence. Hence, owing to the requisite virtual and electronic wherewith all, and principally, striving to build a tele-secretariat, and not an orthodox standard office, the budgets shall be austere, and size of the personnel lean, not to encumber the tax payers. The Council's forte would be to deliver through professional acumen; seeking improvisation, adjustment and relocation of existing assets, resources and personnel from the Government; and Community participation and public and private partnership.

(2) The Council shall, under the existing rules, submit a modest budget proposal for requisite Fund to the Government of Pakistan.

(3) The Fund shall be administered by the Council with oversight exclusively from the Senate Standing Committee on Defence with the Secretary, Finance Division, as Chair of the oversight sub-committee, which shall have the power to audit the accounts, in addition to the external audit conducted by the Auditor General of Pakistan.

(4) Funding shall only be approved by the Council to support initiatives that develop, coordinate and implement the Cyber Security policy.

MISCELLANEOUS

12. Overriding effect.- The provisions of this Act shall have effect notwithstanding anything to the contrary contained in any other law.

13. Immunity of the Council and its Employees, etc.-No suit or other legal proceedings shall lie against the Council or any officer or employee thereof or any person acting under its direction:

(a) for any act done in good faith,-

(i) in the performance, or intended performance, of any function or duty; or

(ii) in the exercise, or intended exercise, of any power, in the capacity of the Council under this Act; or

(b) for any neglect or default in the performance or exercise in good faith of such function, duty or power.

14. Savings of Armed Forces and Intelligence Services Powers.- (1) This Act shall be without prejudice to the activities, powers and functions of the Armed Forces or intelligence agencies or services and shall be without prejudice to the operation of or powers exercised under-

(a) section 54 of the Pakistan Telecommunication (Re-organisation 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; and
(f) any other intelligence agency or service that does not itself undertake the investigation or prosecution of any criminal offence.

15. Removal of difficulties.-The Federal Government may by notification in the official Gazette, make provisions for removal of difficulties in a manner not inconsistent with the provisions of this Act.

SCHEDULE 1

1. Establish an independent National CERT under private public partnership.

2. Assist in the establishment of industry and sector specific CERTs.

3. Subject to privacy, corporate confidentiality, intellectual property and National security establish a voluntary mechanism, with legislative incentive if necessary, for sharing of Cyber Security related information and data between the private sector and public sector.

4. Establish an Accreditation and Standardization Mechanism for Public Sector Critical Information Infrastructure;

5. Prepare and issue a National Cyber Security Strategy and an International Cyber security Strategy;

6. Facilitate the establishment of a Cryptographic Product Evaluation Laboratory.

STATEMENT OF OBJECTS AND REASONS

Given the clear and present danger of threat to Pakistan's national security via cyber warfare, as demonstrated by revelations of intrusion into privacy and spying by overseas intelligence network, and given the context that cyber warfare is currently being weighed actively in the region where Pakistan is located, it is imperative that Pakistan take institutional steps to combat this threat.

In my capacity as Chairman of the Senate Defence Committee, a number of initiatives were launched including a Policy Seminar on Cyber Security, the establishment of Cyber Security Task Force and the publication of a manual for the media on cyber security. However, there is a need to establish a broad-based institutional mechanism regarding cyber security and it is in this context that I am introducing the National Cyber Security Council Bill, 2014.

SENATOR MUSHAHID HUSSAIN SYED
Member-in-charge