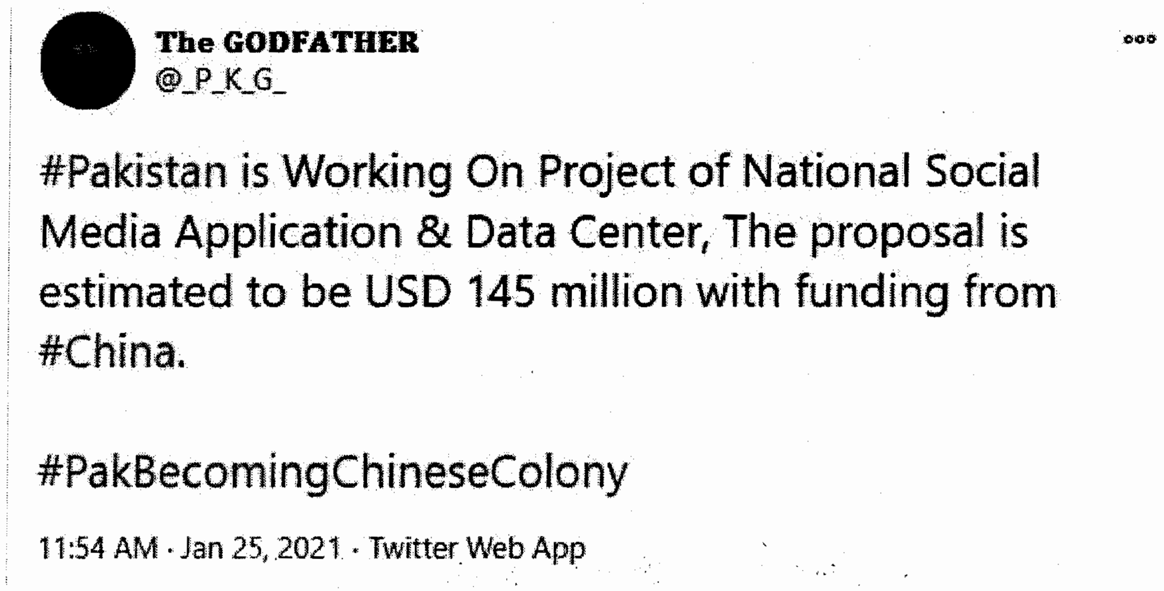
Subject: **Advisory – Planning Commission-Leaked Documents (Advisory No.4)**

1. On 25 January 2021, an Indian Hacker on Twitter shared sensitive documents **(Annexure- A)** of Planning Commission indicating a Cyber Security violation. Initial analysis revealed likely existence of **sophisticated malware** in **Planning Commission IT systems** connected with Govt offices / ministries.

2. Moreover, occurrence of similar Cyber Security breaches at other key ministries have also been observed with **presence of specially crafted malware.**

3. Above in view, it is recommended to adopt **preventive measures** and **implement guidelines** suggested at **Annexure-B.**

Annexure - A



The GODFATHER
@_P_K_G_

#Pakistan is Working On Project of National Social Media Application & Data Center, The proposal is estimated to be USD 145 million with funding from #China.

#PakBecomingChineseColony

11:54 AM · Jan 25, 2021 · Twitter Web App

Annexure-B

GUIDELINES FOR EMAIL SECURITY

1. **Introduction** An email server is a vital part of any IT infrastructure and it is difficult to operate without operational email. However, lack of security practices like encryption, antispam and anti-phishing mechanism, email server may fall prey to hostile elements attempts. Many mail servers operating within sensitive organizations of Pakistan (well reputed government and defense organizations) are observed to be less secure and are under continuous threat of HIA monitoring and interception. Therefore, it is strongly recommended to follow secure email practices to prevent against nation state intrusions.

2. Recommendations for Email Server Administrators.

Following recommendations must be followed in true spirit for prevention against hostile espionage and threats actors: -

a. For secure communication, **email server should be hosted on secure domains with valid / verified HTTPs SSL certificate.** SSL certificate can be obtained from trusted vendors like GoDaddy, GlobalSign or Verisign etc, moreover, free SSL certificates may also be obtained via certificate authorities like LetsEncrypt (letsencrypt.org) or ZeroSSL etc.

b. **To combat against Spamming, Spoofing and Phishing,** enable **SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting and Conformance)** in DNS record.

c. **Anti-spam software's** to be deployed at email server to detect and filter spam.

d. Apply **heuristic and fingerprinting schemes** that cater attack techniques for defence against phishing email and compare samples of previous attacks.

e. Ensure that end user has employed **endpoint security solution** to combat phishing

f. Consider deploying both **inbound filters** and **outbound content filters.**

g. Always verify and test the domain for above configuration **by checking via online websites like dmarcian.com (DMARC Inspector), dkimvalidator.com (DKIM Validator) and mail-tester.com (Spam Test). If email server doesn't qualifies the test then it shouldn't be deployed in production environment.**

h. It is mandatory **to turn on STARTTLS on email servers** and **test it** after deployment and configuration via **https://www.checktls.com/ TestReceiver (Online TLS Checker).** If any of the **test fails then email server shouldn't be deployment in production environment.**

3. **<u>Recommendations for Internet/ Email Users.</u>**

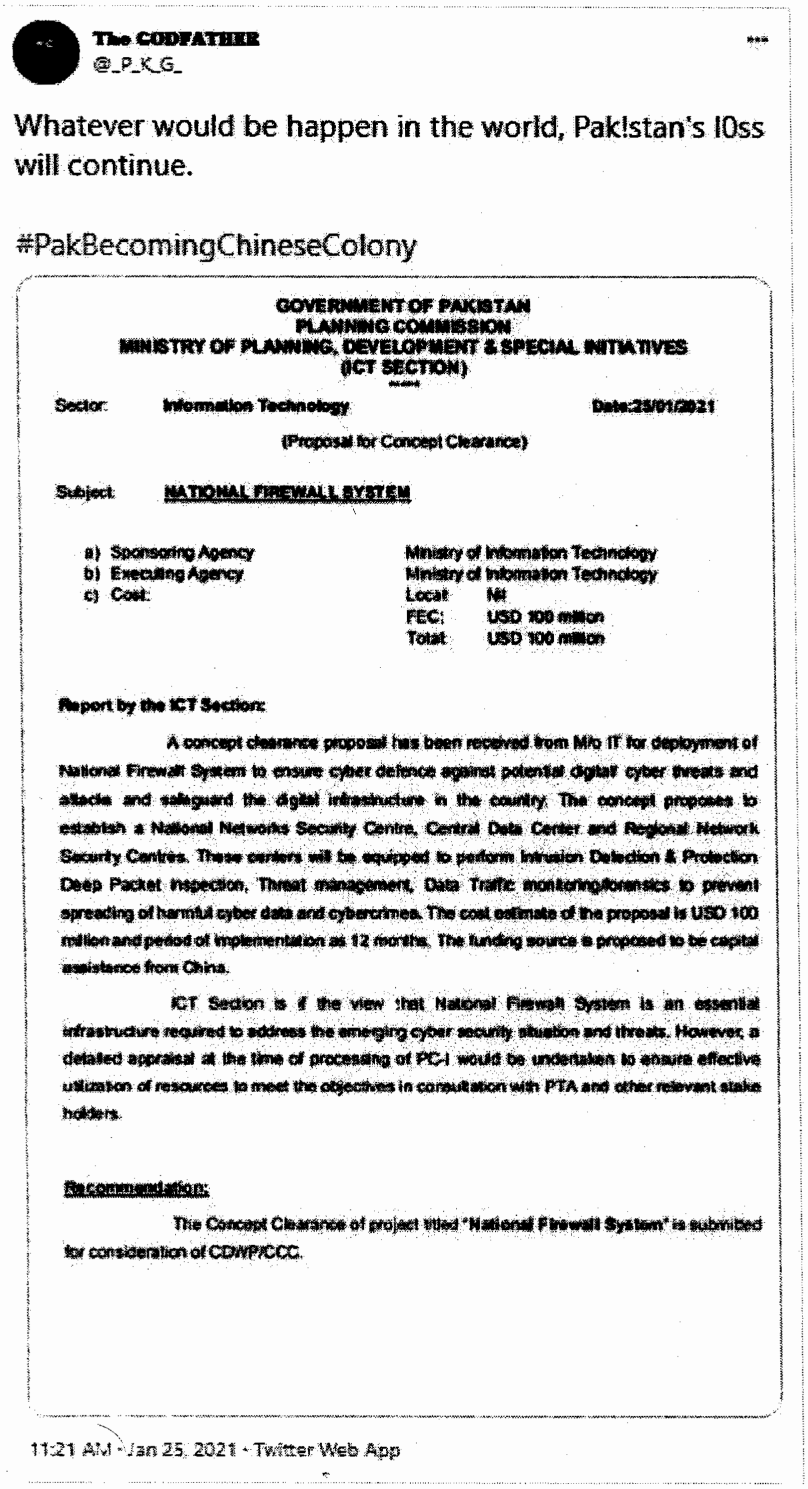
a. All email attachments sent must be encrypted with password and password must be communicated through different media.

b. Always confirm the identity of the individual to whom email is being sent or received.

c. Never open attachments from untrusted sources.

d. Endpoint on which official email is being accessed/ sent should be secured via well reputed, licensed and updated antivirus solution.

e. Never forward your OTP (One-time password) to anyone.



The CODFATHER
@_P_K_G_

Whatever would be happen in the world, Pak!stan's l0ss will continue.

#PakBecomingChineseColony

GOVERNMENT OF PAKISTAN
PLANNING COMMISSION
MINISTRY OF PLANNING, DEVELOPMENT & SPECIAL INITIATIVES
(ICT SECTION)

Sector: **Information Technology** **Date:25/01/2021**

(Proposal for Concept Clearance)

Subject: **NATIONAL FIREWALL SYSTEM**

a)	Sponsoring Agency	Ministry of Information Technology	
b)	Executing Agency	Ministry of Information Technology	
c)	Cost:	Local	Nil
		FEC:	USD 100 million
		Total	USD 100 million

Report by the ICT Section:

A concept clearance proposal has been received from M/o IT for deployment of National Firewall System to ensure cyber defence against potential digital cyber threats and attacks and safeguard the digital infrastructure in the country. The concept proposes to establish a National Networks Security Centre, Central Data Center and Regional Network Security Centres. These centers will be equipped to perform Intrusion Detection & Protection Deep Packet Inspection, Threat management, Data Traffic monitoring/forensics to prevent spreading of harmful cyber data and cybercrimes. The cost estimate of the proposal is USD 100 million and period of implementation as 12 months. The funding source is proposed to be capital assistance from China.

ICT Section is if the view that National Firewall System is an essential infrastructure required to address the emerging cyber security situation and threats. However, a detailed appraisal at the time of processing of PC-I would be undertaken to ensure effective utilization of resources to meet the objectives in consultation with PTA and other relevant stake holders.

Recommendation:

The Concept Clearance of project titled "**National Firewall System**" is submitted for consideration of CDWP/CCC.

11:21 AM · Jan 25, 2021 · Twitter Web App