Subject: - **ADVISORY REGARDING SPEAR PHISHING E-MAILS FROM HACKED GOVERNMENT WEBSITES**

1. Recently, there has been an increase in cyber-attacks on government websites of Pakistan. In addition to defacement and DDoS attacks, it is likely that various databases / mail servers have been compromised.

2. **Recent Incidents**. In August and September 2014, various malware with spear phishing emails have been received and analyzed which revealed following new dimensions of cyber threats to compromise IT systems/computers:-

- **a.** Spear phishing emails originated through hacked email accounts of Prime Minister' s office are being used to spread malware.
- **b.** Use of dynamic DNS instead of static IP / URL as C&C server to avoid IP blocking/mitigations at national gateways .
- **c.** Use of latest/ zero-day exploits like MS word/ flash player, acrobat to infect the system.

3. **Recommendations.** Keeping above in view following is recommended:-

- **a.** It is suggested that thorough vulnerability assessment and auditing of web and email servers be conducted through network security professional.
- **b.** Conduct comprehensive forensics to identify hacking/misuse of official email accounts by validating user of active directory services.
- **c.** IT and IT security polices of various government departments and ministries require revision. Procedures need to be streamlined for creation of official email addresses and their modification / deletion on change of appointments.
- **d.** Necessary security training of technical staff may be conducted.

e. Cyber security awareness / training for end user by respective departments be conducted regularly

f. Due to sensitivity of information, the physical and network security infrastructure be reviewed and enhanced, so that leakage of sensitive information be prevented in future.

g. Network security capability services provided by network operators may be reviewed to prevent from such activities in future.

h. In addition to traditional network security mechanism, latest solutions like NG Firewall, Malware Protection System, End Point protection, providing web hosting facilities/ services especially to Government/departments.

i. Expertise/training level of NW Administrator /Security Analyst may also be reviewed /ascertained being a sensitive task /nature of services.

j. Avoid downloading emails attachments from unknown as well as known / legitimate sender unless confirmed.

k. It is imperative to update software like Windows Operating System, Microsoft Office package, Java, Adobe Flash Player, Adobe Reader etc. on regular basis.

l. Install and regularly update firewall and antivirus softwares.

m. Avoid using VPN software such as spot flux hotspot shield .