Subject: - **Advisory Directive - Prevention against Cyber Espionage**

The increasing volume and sophistication of cyber security threats-including targeting phishing scams, data theft, and other online vulnerabilities-demand strict vigilance and security measures on IT users and systems / assets. This fact even gets more pronounce under existing security threat environment and with ongoing process of improving IT systems application with ever changing technology and with improper security control mechanism in place. The IT resources held with various organizations mostly in the public and private is unprotected primarily due to continuous hacking attempts adopted by hostile agencies using new attack methods, thus invariably increasing risks on every web user. A number of such threats have been reported through reliable sources to have attacked our sensitive installations / data centers using smart phishing techniques, defining type of threat, mode and probable implications on our national security. Summary of threat analysis, malware type, modus operandi and measures to mitigate such emerging threats has been attached as '**Annex A'** to this letter.

2. Foregoing in view and sensitivity of the matter besides prevailing security environment of our country, all intended users and managers of federal ministries, divisions and provincial govt bodies, affiliated / attached govt departments are requested to critically examine, disseminate and educate all such measures to their officers as well officials employed on such duties.

3. It is requested that this information may be disseminated to all organization/ department /users under your control for appropriate precautionary and preventive action as per Annexure **'A'**.

No. 1-5/2003 (NTISB)-II Dated December, 2014 **Annex 'A'**

Ser	Type of Threat	Intended Targets	Malware Information	Threat Analysis	Preventive Measures
1.	Spear-phishing emails	Government officials and sensitive organizations.	Various spear-phishing emails are being received by users of government and sensitive organizations. Subject emails contain various types of malware / exploits, Following are the reported emails. **a.** Pakistan to sell fighter jets to Sri Lanka **b.** Big lie of India exposed for cross border firing **c.** How do we protect our self against Ebola **d.** The mujahid injuries and deaths in North Waziristan.	Specially crafted Microsoft Word and power point files which open a document seamlessly and execute malware in the background, aimed at stealing sensitive information and taking full control of computers.	**a.** In case any such file has already been opened by any user ,it is recommend that system be reinstalled or restored to previous backup. **b.** No such malicious emails received be opened and may be reported to this organization on email address. (**shikra343@gmail.com**)for analysis and
2.	Dark hotel Malware	Senior level executives from large global companies while staying in luxury hotels.	A seven-year-old cyber espionage campaign has targeted senior level executives from large global companies by using specialized Advanced Persistent. Threat (APT), zero-day exploits, and well-developed key loggers to	The targets are lured in using bogus software update for adobe Flash, Google Toolbar or Windows messenger which contain malware. Malware installs key loggers and tracking application to infected	**a.** Be very careful while using public Wi-FI network / free hotspots. **b.** Instead use own mobile device as hotspot to

			extract information from them when they stay in luxury hotels during their business trips. The group has been operating in Asia since 2009 but there have been infections recorded in the United States, South Korea, Singapore, Germany, lreland and many other countries, as well. It uses hotel WI-Fi networks to target elite executives from manufacturing, defense, investment capital, private equity, automotive and other industries. The group has access to zero day vulnerabilities and exploits and it used them to infect victims. Threat actors use three different malware distribution methods;- **a.** Malicious WI-Fi networks. **b.** Booby –trapped P2P torrents. **c.** Highly customized spear phishing.	users through out the World. The darkhotel malware operating group uses weak digital certificates to sign their malware.	avoid using bogus Wi - Fi networks. **c.** Never install any offered update when accessing internet from un-trusted connection.

3.	Line Messenger/ Line App	-	“Line” is a Japanese proprietary application for instant messaging on smart phones and personal computers “Line” users exchange text messages , graphics, video and audio media, make free VoIP calls, and hold free audio or video conferences . “Line” launched in Japan in 2011, reached 560 million users worldwide and is available on Android, iOS, Windows and Firefox OS for mobile and Mac OS for computers.	Serious vulnerability was found in “Line” App’ which identified that the app turned off encryption when on cellular data. Voice message are uploaded via plain http in an unencrypted m4a format. In addition, status updates, timeline post, comments to those posts , users IDs, chat messages and server login tokens are all clearly visible in plain text. These could easily be reconstructed by a man-in-the-middle attack phones while inside the mobiles operator’s network on internet backbone.	All concerned be advised to avoid downloading/using “Line” messaging app till the time it is properly evaluated and vulnerabilities are not fixed.