Subject:- **Use of Web Applications – Viber (Advisory No. 03 – February, 2015)**

Viber is the most downloaded applications on various mobile application stores. There are serious security issues found in the Applications. Detailed analysis is given below:-

a. **Company Background.** Viber Media was founded by four Israeli partners. Talmon Marco, Igor Megzinik, Sani Maroli and offer Samocha, with Talmon Marco as its CEO. Viber was initially launched for iPhone on December, 2, 2010 , in direct competition with Skype. Viber has over 100 million monthly active users from its 280 million users. Japanese e-commerce giant Rakuten acquired Viber Media for $900 million in Feb.-2014.

b. **Viber Media's Source of Investment.** Founders of Viber are associated to the Israel Defense Forces. Viber Media is controlled from Israel and its development is outsourced to Belarus. The strangest part in Viber Media's story is that the company was funded by individual investors, who Marco described as "friends and family". A huge investment of $20 M had been invested in the company, as of May 2013.

c. **Viber App Brief.** Viber application is used to send free messages and make free calls to other Viber users, to any device and network, in any country.

d. **Cyber Security Concerns regarding Viber.**

(1) **Viber's Privacy Policy**

(a) A copy of the phone's address book & call detail record are stored on Viber server.

(b) Location information is stored on Viber Servers.

(c) Viber can share or disclose collected user information to comply with their trusted law enforcement agencies.

(2) **Viber can perform following actions on a mobile:-**

(a) Read phone status and identity.

(b) Read your text messages (SMS or MMS)

(c) Record audio.

(d) Approximated location (network-based)

(e) Precise location (GPS and network-based)

(f) Read call clog.

(g) Read our contacts.

(h) Read our social stream.

(i) Modify or delete the contents of your USB storage.

(j) Find accounts on the device

(k) Read Google services configuration.

(l) Use accounts on the device.

(m) Change network connectivity.

(n) Full network access.

(o) Google Play billing service.

(p) View Wi-Fi connections.

(q) Retrieve running applications.

(r) Read sync Setting

(s) Modify system settings.

(t) Test access to protected storage.

e. **Security Flaws in Viber Applications.**

(1) According to a security flaw identified in 2013, Viber gets hacked through special SMS and subsequent actions.

(2) On November, 4, 2014 Viber scored 1 out of 7 points on the Electronic Frontier Foundation's secure messaging scorecard because of weak encryption.

f. **Security Analysis.** Following serous security concerns are identified in Viber:-

(1) Viber applications reads private information from mobile such as contacts , call logs, sms, location etcetera and sends the information to its servers.

(2) Viber media doesn't have known investors therefore it is highly likely that it may be a state sponsored applications which is capable of monitoring every activity of a users.

(3) Unwary user's leak sensitive /personal information about their friends e. g a person saves contact details of his friends as "Maj Ali , Sec-xxx , ISI Military , Navy or Air Force unit". Such practice helps viber in identification of a security conscious individuals who don't share their information online.

(4) Viber uses a number of unauthorized techniques including Cookies , clear GIFs and other automatic data collection techniques to spy & track its users.

2. **Recommendations.** Keeping above it is strongly recommended that Viber may not be used by any official users /sensitive appointments or if unavoidable a separate mobile be used for the purpose.