Subject: **Advisory - Prevention against Indian Oriented Offline Maps Mobile Application - Deesha (Advisory No.94)**

1. **Introduction.** Recently, it has been observed that an **Indian origin 3rd party Android navigational application "Deesha"** is being used for offline road navigation. The application is not available on Google Play store and may be downloaded from 3rd party servers. Users feedback of the application is quite positive, hence, its large scale usage in future cannot be ruled out.

2. **Features - Deesha Application.** The application automatically gets access to host system, data store, SMS read and location permission without prior knowledge of the users. Additional features of the application include; displaying location in Indian Grid System with accuracy, navigation to save way points, photo geotagging, location sharing, map view with panning and zooming option and displaying device way points. Computation of location is independent of availability of internet / mobile network. As **Deesha** is an Indian 3rd party app, hence, under command organizations / users may be instructed to refrain from its use. Few best practices / recommendations to be adhered to while downloading / using mobile applications are mentioned at **Para 3.**

3. **Best Practices / Recommendations for Mobile Application Usage**

a. **Block all applications installs from unknown sources**, these options are disabled in Android by default and it should stay that way.

b. Only install application form official App Stores / Google **Play Store.**

c. **Google Play protect** (Android built in Anti Malware) **must not be switched off** in any case. It detects suspicious looking apps in your mobile device based on their behavior and generates alerts for user.

d. **Do not click on links that promise unusual features or functionalities** such as **"WhatsApp offers of free Airline Tickets"** are usually just an attempt to steal your personal data. The same applies to phishing including texts from friends containing suspicious URLs.

e. Before installing any application, **user must read its privacy policy explaining what data it is collecting form users and with whom it is sharing that data.**

f. It is strongly recommended to all users to ensure keeping their **communication app up-to-date from their respective App Stores. Do not ignore updates from apps installed on your device.**

g. **Regularly Update Mobile Operating System** whenever updates are available.

h. **Use of mobile Antivirus** in order to prevent any danger that may affect your Personal data on device.

i. **Carefully consider what information you want to store on the device,** remember that with enough time, sophistication and access to the device, any attacker can obtain your stored information.

j. **Be careful when using social networking apps;** these apps may reveal personal information to unintended parties. Be especially careful when using services that track your location.

4. Disseminate the same to attached / affiliated, Departments and Branches, forwarded for necessary action, please.

5. **Reporting of Suspicious Files / Emails.** Any malicious activity may be reported to this organization on the following email address for analysis and suggesting mitigation measures: -

asntisb2@cabinet.gov.pk