Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No 41) July 18**

1. Introduction. A **critical vulnerability** has been found in "Cortana" an **artificial** intelligence-based smart **assistant** that **Microsoft** has built into all versions of Windows 10, allow cyber criminals to **unlock** your **system password** and **access** the **system.**

2. Technical analysis

a. The vulnerability can **retrieve** information from **Cortana, start an application** from the **Windows lock screen,** and even **log** into a Windows without a user interacting with the computer.

b. Hackers could also **compromise** the system completely if the user has **elevated privileges** on the targeted system.

c. Vulnerability details are as under: -

(1) CVE Number. CVE-2018-8140.

(2) Vulnerability Impact. Cortana **Elevation of Privilege** Vulnerability.

3. **Affected Product Versions.** This critical vulnerability affects virtual assistant **"Cortana"** in windows 10.

4. **Mitigation Measures.** Following best practices are suggested in this regard:-

a. It is advised to immediately **turn off** Cortana on the **lock screen.**

b. Microsoft has released **security patches** against this **vulnerability** so it is recommended to **update** your windows 10.

5. **Recommendations.**

a. Regularly check the **company website** for **updates** and release of **security patches.**

b. Strictly follow all **mitigation** measures discussed at para 4.

c. Install and update well reputed antiviruses such as Kaspersky, Avira, Avast etc.

d. Update all software's including Windows OS, Microsoft Office and disable macros.

e. Don't download **attachments** from untrusted sources.

e. Physical security of all computers and digital device§ should be ensured