Subject: **Prevention Against Cyber Espionage - Advisory No 07 March 2018**

1. **Introduction.** Zero day vulnerability has been found in "Adobe Flash Player" that may allow hackers to take control of the affected system. To exploit the vulnerability, attacker need to trick victims into opening Microsoft Office documents, web pages or spam messages that contain a maliciously crafted Adobe Flash file.

2. **Technical analysis**

   a. These attacks spread via Office documents with embedded malicious Flash Content distributed via email, web pages or span messages.

   b. Vulnerability details are as under:-

      (1) CVE Number - CVE-2018-4878.

      (2) Vulnerability Impact - Remote Code Execution.

3. **Affected Product Versions.** The critical vulnerability affects Adobe Flash Player version 28.0.0.137 and earlier versions for:-

   a. Desktop Runtime (Win/Mac/Linux).

   b. Google Chrome (Win/Mac/Linux/Chrome OS).

   c. Microsoft Edge and Internet Explorer 11 (Win 10 & 8.1).

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

   a. Immediately update Adobe Flash Player with latest security patch issued by **Adobe.**

   b. Be careful while using social media groups/ pages and don't click or download any file or image.

   c. Don't open any document received via email or any unknown resource.

   d. Install and update well reputed and licensed antiviruses.

   e. Keep all the software's, browser and operating system up-to-date.

5. **Recommendations**

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

   b. Strictly follow all mitigation measures discussed at Para 4.