Best Practice Recommendations for Handling and
E-Filing of Confidential Information at the CIT

E-Filing/Retrieving Confidential Documents

1. If an attorney inadvertently files a Confidential document in an incorrect case or on the public CM/ECF System, he/she should immediately notify the Clerk's office so that the document can be deleted from that file.

2. Attorneys retrieving a document containing Confidential information from the Court's CM/ECF System should ensure that the computer on which the document is being downloaded is secure, has up-to-date antivirus protection, and that the document is not accessible by anyone who is not authorized under the Court's Rules to review that document.

3. There should be no back-up (automatic or otherwise) or retention of Confidential documents downloaded from the CM/ECF System other than to a secure server. No Confidential documents retrieved from the CM/ECF System should be placed or retained in emails.

4. Any hard drive, disk, CD, flash drive, or other storage medium used for documents containing Confidential information must be password protected or otherwise accessible only to authorized persons.

5. The copying of all documents containing Confidential information should be regulated. If a copy is made (hard copy, disk, CD, etc.), parties are reminded that they must destroy the copy at the end of the case.

6. It is safest not to remove media containing Confidential information from the office premises of the authorized person to prevent inadvertent loss. When such off-site use is required, necessary precautions to safeguard the information should be exercised.

Passwords/Access

7. Attorneys who will need to file documents containing Confidential information or access Confidential documents under protective order or pursuant to Form 17 must register as a Confidential Information Filer with the Court and change their password yearly. The new password will be used by the attorney for all public and Confidential submissions thereafter.

8. Attorneys should safeguard their passwords carefully and, in particular, should not save or record the password on their computers. Attorneys should not use their passwords on any public terminal, on a private laptop in a public setting, or anywhere

others might be able to learn their password. If there is any concern by an attorney that the password has been compromised, the attorney should revise his/her password and contact the Clerk's Office.

9. When accessing information from a wireless network, attorneys should use a secure wireless connection with robust encryption.

Service

10. No document containing Confidential information retrieved from the Court's CM/ECF System should be sent by email to anyone. No e-filings with the Court containing Confidential information should be sent by email to another attorney as service. Electronic filing of any document and the Court's transmission of Notice of Electronic Filing will constitute service of such document on all counsel who are registered on the CM/ECF System. Authorized attorneys may then access that Confidential document directly from the CM/ECF System.

Agency Restrictions

11. Attorneys are reminded that they remain subject to the rules and procedures governing handling of BPI by the agencies providing access to the Confidential information initially.