

EXTERNAL PROCEDURES REGARDING PASSWORD-PROTECTED SEALED
APPLICATIONS

1. DOJ/USAO opens a case shell in CM/ECF as outlined in the Sealed Application Instructions pursuant to the MOUs. (*Note: the shell should not have any identifying information about the subject of the case.*) No docket entries will be made in the case by DOJ/USAO.
2. DOJ/USAO will email draft password-protected documents (to include the ***motion to designate case and all filings as password protected***¹) to warrants_criminal@dcd.uscourts.gov.² The email should:
 - a. state that the attachment is being submitted pursuant to password-protected protocols;
 - b. include the phone number of the DOJ/USAO employee whom the Court staff can call to learn the password; and
 - c. state whether any proposed changes to the document can be shared with DOJ/USAO via email or should be via phone call.
3. The visiting/duty MJ will relay any edits to DOJ/USAO in the prescribed manner and then direct DOJ/USAO to email the corrected version.
4. The filing will be treated as an afterhours warrant. DOJ/USAO will send the finalized password-protected pleading to warrants_criminal@dcd.uscourts.gov.
5. Once signed, the criminal law clerk will send the signed password-protected pleadings back to DOJ/USAO.

Note: For subsequent filings, please follow the steps outlined above with the exception of the case opening.

¹ The motion, as entitled above, must include a request to designate all filings as password protected, to NOT be placed on CM/ECF, and to remain under seal. This motion is not necessary for subsequent filings.

² 2703(d) applications and related documents do not go through steps 3 and 4.