IN THE COURT OF APPEALS OF MARYLAND
ADMINISTRATIVE ORDER ON THE IMPLEMENTATION OF
ELECTRONIC SEARCH WARRANTS

WHEREAS, Chapter 107 of the 2014 Laws of Maryland (Chapter 107) provides for the electronic submission of an application for a search warrant, the electronic issuance of a search warrant, and the electronic submission of the search warrant return; and

WHEREAS, Chapter 107 further provides that the electronic submission and issuance can be done either through secure facsimile (fax) or secure electronic mail; and

WHEREAS, Amendments to Maryland Rule 4-601 become effective July 1, 2015 and provide for the implementation of Chapter 107; and

WHEREAS, Amended Maryland Rule 4-601 requires the State Court Administrator to designate the electronic text format for the submission of search warrant documents from law enforcement officers; and

WHEREAS, The State Court Administrator has designated the secured PDF as the electronic text format for submission of electronic search warrant documents by law enforcement officers; and

WHEREAS, The Court Technology Committee proposed a uniform procedure to the Judicial Council that would assist judges in ensuring that they maintain an acceptable level of security when receiving and approving search warrants through the electronic medium; and

WHEREAS, The Judicial Council expressed the need to establish standards of security related to the processing of electronic search warrants;

NOW, THEREFORE, I, Mary Ellen Barbera, Chief Judge of the Court of Appeals and administrative head of the Judicial Branch, pursuant to the authority conferred by Article IV, § 18 of the Maryland Constitution, do hereby order this 26th day of June 2015, that

1. The administrative judges in the respective Circuit and District Courts in each jurisdiction meet to develop a protocol for the implementation of electronic search warrants, giving consideration to the procedures drafted by the Court Technology Committee, attached hereto, regarding appropriate security standards for the receipt and issuance of electronic search warrant documents; and

2. In particular, any established protocols that provide for the use of electronic mail as a means for transmission of search warrant documents shall require a written certification from the law enforcement agency indicating that the domain from which the documents are sent is secured by a Secure Sockets Layer (SSL) certificate; and

3. Any established protocols that provide for transmission via fax, shall require all search warrant documents to be sent from a fax machine controlled by the law enforcement agency directly to the judge's fax machine or to a fax machine that, for the purposes of receiving and sending documents related to the search warrant, is controlled by the judge; and

4. Administrative judges shall adopt the secured PDF as the electronic text format for search warrant documents as designated by the State Court Administrator pursuant to Rule 4-601.

/s/ Mary Ellen Barbera
Mary Ellen Barbera
Chief Judge of the Court of Appeals

Filed: June 29, 2015

/s/ Bessie M. Decker
Bessie M. Decker
Clerk
Court of Appeals of Maryland

JUDICIAL COUNCIL

Court Technology Committee

Electronic Search Warrant Procedure

Overview

The General Assembly authorized the delivery of search warrants and related papers[1] by secure and reliable electronic mail and by secure facsimile.[2] The Court of Appeals approved amendments to Rule 4-601 implementing the procedures authorized by the General Assembly.

In order to assist judges in maintaining the required security and secrecy, the Court Technology Committee developed procedures to be considered by judges when accepting electronic search warrants and related papers. The procedures are not intended to require a judge to accept electronic warrants.

Of the two authorized electronic methods, facsimile is the least favored. Facsimile presents issues of security and secrecy. Fax machines do not require passwords and they are frequently placed in common areas so they are accessible to persons other than the intended recipient of a transmission. Before accepting any electronic search warrant, by fax or e-mail, the judge should take whatever steps he or she deems necessary to ensure that the security and secrecy of the warrant process is preserved. In the case of fax, this may include insuring that the recipient is physically present at the fax machine at the time of the transmission.

[1] At a minimum, there must be an application, affidavit and proposed warrant. Additionally, there could be a motion to seal. These procedures apply to all papers related to the issuance of a particular search warrant. The term "search warrant and related papers" shall refer to all such documents.

[2] Crim. Pro §1-203

The issuing judge is ultimately responsible for compliance with the governing rule. The judge should decline to take an electronic search warrant and related papers if the judge believes that he or she cannot receive or transmit the paperwork securely or believes that circumstances require an in person delivery of the warrant.

Recommended Electronic Warrant Procedures

1. It is essential that the law enforcement officer contact the judge to determine whether the court is amenable to receiving an electronic search warrant application by secure fax or secure electronic mail.
2. The judge must take such steps as he or she deems necessary to verify the identity of the officer. If the judge is not comfortable with the identity of the officer or the officer's ability to deliver the warrant and related papers by secure fax or e-mail, the judge should require the warrant and related papers to be delivered in person.
3. To be secure and effective, it is necessary that the judge know what he or she will be receiving and when it will be received. There is added security in receiving an expected electronic transmission, from a known source, containing what was expected, at the time it was expected. Judges should consider these factors.
4. To ensure the secrecy and security of electronic process, it is essential that the means of transmission be to and from the following:
    a. In the case of e-mail, the e-mail must be sent from an official law enforcement domain that has a Secure Sockets Layer (SSL) certificate[3].

[3] The Committee suggests that the law enforcement agency should be required to provide a written certification that they comply with this requirement before warrants are accepted from the agency.

The officer must use the officer's official agency e-mail account and his or her agency has determined to be secure. The officer must send the e-mail to the judge's official e-mail account. The judge must return the warrant to the officer's official, secure, agency e-mail address via the judge's official judiciary e-mail account or a secure e-mail client contained within the program provided by the Judiciary for applying the electronic signature. Adobe EchoSign is secure.

b. In the case of fax transmission, the officer must send the warrant and related papers from a fax machine controlled by the officer's agency to the judge's personal fax machine or a fax machine controlled by the judiciary. The parties should arrange for the recipient to be present at the fax machine to receive the transmission personally.

5. If the warrant and related papers are sent by e-mail, the complete text of the application, affidavit and search warrant shall be sent in PDF format that is editable using Adobe Pro. If possible, the officer should send the warrant in a PDF file format that is password protected and encrypted.[4] If the officer does not have that capability or, if the judge is unable to open and edit the password protected, encrypted PDF, the file may need to be resent in simple PDF format. All documents should be in one file.

[4]Microsoft Word has the functionality to save a file in this format. The Committee believes that other popular word processing programs are also likely to have this functionality. The Committee has not been able to test all available programs. The password should be provided to the judge at the time the officer and the judge speak on the phone. The password should not be included in the email.

6. If a warrant is submitted by facsimile, the signed application, supporting affidavit, and the proposed search warrant must be sent to the judge in triplicate[5]
7. The affidavit must be signed and dated prior to transmission to the judge. If not signed, it can be resubmitted after being signed by affiant. Additionally, the application must be affirmed under the penalties of perjury to be true and set forth a declaration that the facts contained within are based on the personal knowledge of the affiant that there is probable cause pursuant to Criminal Procedure §1-203 and Maryland Rule 1-202. Judges are reminded that under Criminal Procedure §1-203 the application is required to be "sworn" and the affidavit must contain facts within the officer's personal knowledge that there is probable cause. There is no personal knowledge for the application. There is a personal knowledge requirement for the affidavit of probable cause.
8. The judge may discuss the search warrant with the applicant in person, by telephone, video conferencing[6], or other electronic means. The discussion between the applicant and the judge may be explanatory in nature but may not be for the purpose of adding or changing any statement in the affidavit. Any facts that are not contained within the "four corners" of the warrant should not be considered. If additional facts are considered, the officer should incorporate those facts and resend the affidavit prior to the warrant being signed by the judge.
9. The judge should review the warrant and make changes, if any, by strikethroughs or insertions of text into the warrant.

[5] The Technology Committee may ask the Rules Committee to consider proposing to the Court of Appeals that the rule be amended to eliminate the requirement for triplicate copies in the case of fax transmission.
[6] While the statute specifically permits video conferencing, not all video conferencing is secure. The Committee advises caution.

10. If approved, the judge should sign and date the warrant using a digital signature program supplied by the Judiciary and affix the time of the issuance on the warrant. EchoSign will provide the time and date as part of the signature.
11. Once executed, the judge should e-mail or fax the signed warrant, together with copies of the application and the affidavit, back to the officer. If e-mail is used, the warrant must be in a non-editable form.
12. The judge must preserve and retain a copy of the search warrant and related papers in a secure setting and print at first available opportunity. Documents signed by Adobe EchoSign are available to the judge via EchoSign until the destroy date set for the EchoSign account or until deleted by the judge. The destroy date will be set by JIS, and it will be no less than 30 days from the date of signing.
13. The judge must retain a printed copy of the application, affidavit and warrant until the warrant is returned, executed or unexecuted.
14. The officer shall file a return of the search warrant, either to the chambers judge or directly to the judge who executed the search warrant. If the return is received by the chambers judge, the chambers judge shall transmit the return and inventory of seized items to the original issuing judge.
15. Once a return of the search warrant is received, the printed signed and dated warrant and the printed inventory report and return shall be filed with the clerk of the court.