A. **Purpose:**

To outline the steps on receiving CyberTips from NCMEC, verifying the authenticity of the report, assessing the severity, conducting open-source intelligence (OSINT) and assigning the report to the appropriate law enforcement agency.

B. **Responsibility:**

ICAC Intelligence Analysts

C. **Definitions/Abbreviations:**

Refer to ICAC SOP-02 - Definitions and Abbreviations.

D. **Procedure:**

1. **Accessing IDS and Opening a CyberTip for Review**

1.1 Login to the ICAC Data Systems portal by browsing to www.icacdatasystem.com.

A. Utilize your registered account information to include your email and password for successful login.
B. Authorize IDS to send you an email or text message with a pin to authorize your login
C. Once the PIN has been received, check off "I agree" and enter PIN number. Select "submit".

1.2 On the left side of the homepage, you will see a blue task bar.

A. Select the "Case Referrals" drop down menu
B. Select "Case Referral Dashboard"

1.3 The Case Referral Dashboard defaults to sorting the CyberTips by "created" date. The newest case assignments from NCMEC are at the top of the dashboard.

A. In order to filter out the unnecessary CyberTips from the dashboard, select the three horizontal lines under the "status" column.
B. Ensure the only button that is left unchecked is "Closed". The remaining buttons should all be checked.

1.4 Once filtered, scroll down/browse backward in dashboard pages until you see the lowest "New" status CyberTip in the dashboard. This is where you will start your CyberTip evaluations.

1.5 Select the "case jacket" icon under the "Manage" column on the row of the CyberTip you would like to review. This will open the CyberTip.

2. **Review of NCMEC CyberTips:**

2.1 Before starting your review, select the "Assignments" tab. To ensure another analyst does not duplicate efforts, assign the CyberTip to yourself. As an Analyst/Commander in the system, your name should auto populate in the "members assigned" list along with the other Commanders.

A. Click the "Trash can" button for all other Commanders to remove them from the "members assigned" list until solely your name remains.
B. Click "Save"

2.2 Open the "ICAC SOP 04 - CyberTip Triage Evaluation Worksheet" found in the Division of Scientific Services S:/001 CyberTip Tracking > Standard Operating Procedures folder. Fill out each section as you navigate through your review.

A. Please ensure you fill out this worksheet for each CyberTip review conducted. This will ensure we track our reasoning for each CyberTip action.

2.3. For a quick glance of the CyberTip Triage Evaluation, please open the "ICAC SOP 03 – CyberTip Triage Evaluation Flowchart" found in the Division of Scientific Services S:/001 CyberTip Tracking > Standard Operating Procedures folder.

2.4 Open each "ESP Reported File" provided by the Electronic Service Provider under the "File Type" column.

A. Review each file tag under the "Tags" column on the dashboard. These tags are assigned by a certified NCMEC Analyst. These tags provide an idea of what to expect in the file. However, you must still use your professional judgement.
B. While reviewing each file, determine how to categorize each file. Some examples of categorizations would be:
    a. CSAM – file meets statutory requirements for CSAM possession, distribution, etc.
    b. Age Indeterminate - Unable to determine if the individual seen in the reported file is a minor based on their physical appearance.
    c. Adult – file that depicts an adult with no child present.
    d. Lack of Information – Not enough information provided in the report to assign to a jurisdiction for further investigation.
    e. Self-Production – file was produced by the individual seen in the reported file.

f. Viral – a file that depicts content that is typically shared out of moral outrage or concern for the child’s well-being and spreads rapidly through the internet.

g. Meme/Comedic - a file that is typically shared for comedic affect and bad humor.

h. Unable to Locate – Unable to determine a jurisdiction via OSINT and the CyberTip.

i. Account Compromise – the reported account has been compromised by an unauthorized user.

C. If the files reviewed contain CSAM, the analyst should begin their OSINT using specialized tools, such as Cobwebs/Tangles and TLO, the NCMEC CyberTip and techniques to gather information related to the reported suspect (see ICAC Appendix A – Open Source Intelligence Tools).

a. The analyst should utilize publicly available sources such as social media platforms and websites. The analyst should also utilize law enforcement specific databases such as COLLECT, sex offender registry, NexGen and ICACCOPs.

D. Once OSINT has been completed, any relevant information found should be included in the “Summary of Analysis” portion of the worksheet and documents/notes should be uploaded into the case in IDS.

E. Based off of any relevant information found within OSINT and the NCMEC CyberTip, the case in IDS should be made available to the appropriate law enforcement agency.

3. **Assigning a case to Law Enforcement:**

3.1 Assigning a case to an affiliate through IDS:

A. Click “assignments”, ensure “to individual users” is selected.

B. Under “Add/Remove Access:” type the town you are sending the report to.

C. Check the boxes of the affiliate names, select “Grant Access” and click “SAVE”

D. The “Case Status” at the top left will change to ‘Assigned’.

3.2 Assigning to a CCU State Police Detective through IDS:

A. After your investigation, if the tip resolves to a resident trooper town, assign the tip to the ICAC commander and all the CSP CCU Detectives.

B. Refer to the Resident Trooper Towns document (see ICAC Appendix B – Resident Trooper Towns).

3.3 Assigning to a non-affiliate:

A. Burn a disk with the CyberTip report, reported files and all supporting OSINT information that is relevant to the investigation.

B. Print and attach an official letter head to accompany the burned disks. Ensure you are updating the header to the proper Chief of Police. This is found in S:\001 CyberTip tracking, subfolder “Non-Affiliate Letters”.
   a. Official Letter to solicit non-affiliate – used **only** if this police department has never received a CyberTip before.
   b. Official Letter to Accompany Non-Affiliate – used if this police department has received prior CyberTips via burned disks.
   c. Affirmative Defense Official Letter to Accompany Non-Affiliate – sent when the tip does not meet state CSAM statutes (Sec. 53a-196g)

C. In document titled “CyberTip Labels OK”, add the CyberTip number and print on white CD labels.

D. Place disk in a CD window envelope and secure with evidence tape.

E. Access the OneDrive “Non-Affiliate Tracking” excel document and fill out the columns with the case information.

F. Notify the trooper assigned to delivering the CyberTips by sending them an email containing the CyberTip report number and non-affiliate it is assigned to.