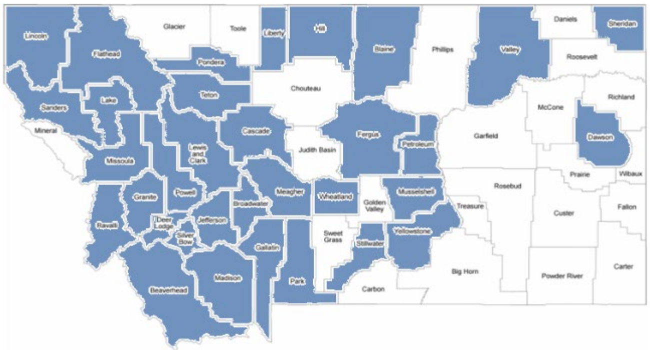
Montana Department of Justice
Division of Criminal Investigation

Computer and Internet Crime Unit

Montana law enforcement continues to expand the utilization of the Division of Criminal Investigation's (DCI) Computer and Internet Crime Unit's (CICU) resources. This document is a response to questions received from the Interim Budget Committee Section D from the December 2023 meeting.

Local Law Enforcement Submitting Cases to CICU from 2022 - 2023



2022 STATISTICS[1]

Staffing: Two (2) Forensic Examiners/Agents

Submitting Agencies: 35 (see Appendix 1)

Case types: Incest, Kidnapping, Possession of Child Sexual Abuse Material (CSAM), Solicitation of a Minor, Sexual Intercourse Without Consent, Sexual Abuse of Children, Homicide, Attempted Homicide, Elder Abuse, Aggravated Promotion of Prostitution, Prostitution, Indecent Exposure, Drugs, Resisting Arrest, Tampering with Witness, Family Violence, Insurance Fraud, Game Violation, Theft, Criminal Mischief, Disorderly Conduct/Obstruction, and an Accident Investigation.

Total cases[2]: 74

- 32 cases were completed in an average of 135 days.
    - 13 cases are "Open and Closed" with an average of 142 days to complete.
        - The device was unlocked, or a passcode was provided when the device was received by CICU. The device data was extracted and analyzed by staff.
    - 14 cases are "Unlock" with an average of 142 days to complete.
        - The device was locked when it arrived at the CICU, and an examiner used a tool to unlock the device. Once the device was unlocked, any of the following steps were completed based on the request:
            1. Device was returned to the requesting agency.
            2. Data was extracted from the device, and everything was returned to the requesting agency.
            3. Data was extracted from the device, the data was parsed using forensic software, and everything was returned to the requesting agency.
            4. Data was extracted from the device, the data was parsed using forensic software, the data was analyzed by an examiner, and everything was returned to the requesting agency.

[1] These statistics include both computer forensic cases and Internet Crimes Against Children cases.

[2] Each case submission may contain multiple pieces of evidence.

    - 5 cases are “Dead” with an average of 100 days to complete.
        - The device arrived at the CICU in a state in which the data could not be accessed. This could be the result of too many incorrect passcodes being entered or the device not yet being supported by the unit’s technology, and the requesting agency asked for the device back.

- 42 cases are “Pending” in the unit.
    - The device is in the queue for forensic examination, software is actively being used to unlock the device (this can take up to 23 years) or the device is not yet supported, and the requesting agency asked the CICU to hold onto the device in hopes it will be supported in the future.

2023 STATISTICS[3]

Staffing: Two (2) Forensic Examiners/Agents first half of year. Four (4) Examiners the second half of the year; one (1) is non-sworn.

Submitting Agencies: 32 (see Appendix 1)

Budget: A mixture of a federal ICAC grant and General Funds; FY2023 = $704,467.02 (see Appendix 2)

Case types: Sexual Abuse of Children, Possession of CSAM, Stalking, Kidnapping, Human Trafficking, Homicide, Attempted Homicide, Sexual Intercourse Without Consent, Drugs, Possession Stolen Property, Assault, Theft, Witness Tampering, Negligent Homicide, Death Investigation, Game Violation, Assault on Police Officer, and Official Misconduct.

Data Processed: 52.25 TB of data which equals 53,504 GBs

Total cases[4]**:** 96

- 35 cases were completed with an average of 70 days.
    - 19 cases are “Open and Closed” with an average of 69 days to complete.
        - The device was unlocked or a passcode provided when the device was received by CICU. The device data was extracted and analyzed by staff.
    - 15 cases are “Unlock” with an average of 68 days to complete.
        - The device was locked when it arrived at the CICU, and an examiner used a tool to unlock the device. Once the device was unlocked, any of the following steps may be completed based on the request:
            1. Device was returned to the requesting agency.
            2. Data was extracted from the device and everything was returned to the requesting agency.
            3. Data was extracted from the device, the data was parsed using forensic software, and everything was returned to the requesting agency.

[3] These statistics include both computer forensic cases and Internet Crimes Against Children cases.

[4] Each case submission may contain multiple pieces of evidence.

        4. Data was extracted from the device, the data was parsed using forensic software, the data was analyzed by an examiner, and everything was returned to the requesting agency.
    - 1 case is “Dead” and took 96 days to complete.
        - The device arrived at the CICU in a state in which the data could not be accessed. This could be the result of too many incorrect passcodes being entered or the device not yet being supported by the unit’s technology, and the requesting agency asked for the device back.
- 61 cases are “Pending” in the unit.
    - The device is in the queue for forensic examination, software is actively being used to unlock the device (this can take up to 23 years) or the device is not yet supported, and the requesting agency asked the CICU to hold onto the device in hopes it will be supported in the future.

DCI is unable to provide the number of all computer forensic cases that were processed in the CICU and referred for federal prosecution. Once the forensic analysis is completed and all evidence is sent back to the investigating agency, DCI does not have visibility on the prosecution unless called to testify to their analysis.

2024 CICU STAFFING

Three (3) Forensic Agents
Two (2) ICAC Agents
One (1) Forensic Analyst
One (1) Program Specialist (modified)

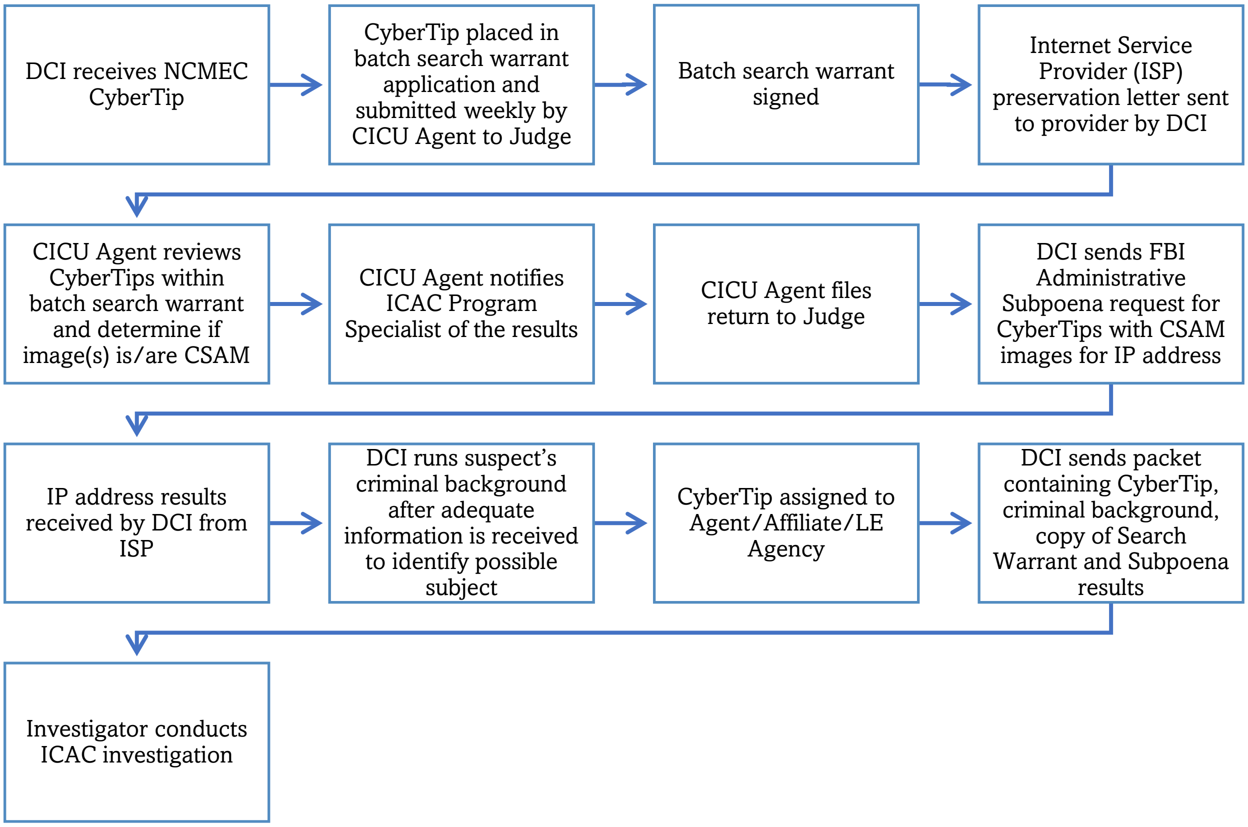
PHOTO, VIDEO, AUDIO ENHANCEMENT CAPABILITIES

In November 2023, DCI moved the photo/video/audio forensics capability to the CICU. This helped to maximize the investment of training, time, and personnel. In November and December of 2023, the unit received eight (8) requests for case support with an average time of eight (8) days for case closure. In 2023, there were nine (9) cases opened and closed in an average time of seven (7) days.

WORKFLOW

An Internet Crimes Against Children (ICAC) CyberTip is generated when an Electronic Service Provider (ESP) identifies illegal activity within their platform that may involve child exploitation, grooming, luring, intent to travel to have sex with a minor, manufacturing child sexual abuse material (CSAM), or possessing/distributing CSAM. The ESP reports this activity to the National Center of Missing and Exploited Children (NCMEC). Once a location is determined for the victim or suspect, the CyberTip is sent to the appropriate ICAC division.

DCI remodeled the CyberTip workflow to bring investigative efficiency and provide a more complete package for law enforcement receiving the information. With this new workflow, DCI can open the CyberTip, consider the offense, and determine the best investigative approach. The workflow consists of the following:


DCI receives NCMEC CyberTip
CyberTip placed in batch search warrant application and submitted weekly by CICU Agent to Judge
Batch search warrant signed
Internet Service Provider (ISP) preservation letter sent to provider by DCI
CICU Agent reviews CyberTips within batch search warrant and determine if image(s) is/are CSAM
CICU Agent notifies ICAC Program Specialist of the results
CICU Agent files return to Judge
DCI sends FBI Administrative Subpoena request for CyberTips with CSAM images for IP address
IP address results received by DCI from ISP
DCI runs suspect's criminal background after adequate information is received to identify possible subject
CyberTip assigned to Agent/Affiliate/LE Agency
DCI sends packet containing CyberTip, criminal background, copy of Search Warrant and Subpoena results
Investigator conducts ICAC investigation

Lawful access

Agents must send a subpoena to the appropriate Internet Service Provider/ISP (ex. cell phone carrier or other ISP) to determine a location of where the Internet was used during the alleged crime, and the identity of the Internet customer. Once determined, investigators may apply for additional search warrants to further investigate the reported activity. A search warrant is sought for all media or data that relates to the suspect's account. This can lead to further information about the suspect's account activity and any other media that could be of evidentiary value.

Suspect location and identity

The exhaustive work of locating the suspect then starts, often taking multiple hours or days. Investigators must also identify who else lives at the residence and establish a pattern of life. The investigator must also verify if the potential suspect has children, access to children, or is employed in a position of trust.

Arrest or search warrant execution

Next, law enforcement must determine if an arrest or search warrant of the residence/person is necessary. Conducting a search warrant on a residence requires a team of multiple law enforcement officers. During a search warrant, investigators typically seize multiple electronic devices; it is not uncommon to find up to 20 electronic devices that need to be examined for evidence.

Forensic Review

Once the forensics are completed on the seized devices, it is imperative that all the evidence is reviewed by the case agent; this could include individually searching through hundreds of thousands of images or videos to locate evidence of CSAM, child exploitation, or other items of evidentiary value. Closely reviewing the communications in a device or account is extremely critical as it could determine the material's origin, identifying more victims, as well as other suspects that are interested in the exploitation of children. It is common to discover chat messages where other account users are communicating about victimizing family members, neighbors, or interested in the distribution and possession of CSAM. This continuation of these investigations could last months to ensure all leads are covered, and any other suspects are identified of victims rescued.

Victims

Investigations of CyberTips can also lead to identifying child victims who have endured sexual abuse and/or have had sexual images produced of them. Investigators may identify victims that may not otherwise have been because of CyberTips. Not only do these victims live within our communities, but ICAC staff identify victims from around the world. Each victim must be located and interviewed, if possible.

CASE EXAMPLES

Many investigations continue beyond the CyberTip or an arrest of the suspect. Refer below:

MT - a suspect was identified following the investigation into multiple CyberTips from online accounts and he was identified as a previous employee of a television network directed toward children. He was communicating with multiple other like-minded individuals about his sexual interest in children, and how he was infatuated with his 8-year-old relative. The suspect also distributed and uploaded multiple images of CSAM to other users. Due to this investigation, several young relatives were identified, and the suspect had direct access to them. DCI staff also found multiple suspects and victims, to include a rape of a 13-year-old, and another allegation of molesting a young relative. This case also led to the identification of a sexual offender distributing CSAM to the suspect from overseas. This investigation took many months as each conversation about the interest in child sexual abuse had to be investigated.

MT – Some investigations turn into multi-year and multi-state cases. In 2022, NCMEC received multiple CyberTips reporting the production of images of the sexual exploitation of a four (4) year old. This case also involved suspicion of the use and sale of narcotics at the same home during the timeframe. The investigation was lengthy because the CyberTip showed an old address where the images of the child were taken; DCI had to investigate the address itself which was a location where people moved in and out on a frequent basis. Eventually, the suspect was located out of state, where he was arrested, and interviewed by Montana DCI. The suspect was brought back to Montana to answer for the crimes. After the interview of the suspect, law enforcement identified another minor victim that he victimized in a third state; ICAC provided the information to law enforcement in that jurisdiction.

MT - DCI is currently assisting a local law enforcement agency with a case that started with 10 CyberTips linked together that have a combined total of approximately 400 videos and images of pre-pubescent CSAM. Through forensic examination, there were only a select few files that looked to be pubescent children. Agents executed a search warrant and seized numerous electronic devices at the suspect's residence, and it became apparent that the subject was possibly manufacturing CSAM. One of the devices seized is a nine (9) terabyte (TB)[5] hard drive which staff are still processing.

[5] 1 TB equals 1,000 gigabytes (GB) or 1,000,000 megabytes (MB).

APPENDIX 1

2022 Agencies Submitting Cases to CICU	2023 Agencies Submitting Cases to CICU
Air Force Office of Special Investigations	Air Force Office of Special Investigations
Anaconda Deer Lodge County Law Enforcement Department	Anaconda Deer Lodge County Law Enforcement Department
Beaverhead County Sheriff's Office	Beaverhead County Sheriff's Office
Blaine County Sheriff's Office	Belgrade Police Department
Broadwater County Sheriff's Office	Cascade County Sheriff's Office
Butte Silver Bow County Sheriff's Office	Colstrip Police Department
Cascade County Sheriff's Office	Dillon Police Department
Conrad Police Department	Division of Criminal Investigation
Division of Criminal Investigation	Federal Bureau of Investigation
Fergus County Sheriff's Office	Fish Wildlife & Parks
Fish Wildlife & Parks	Flathead County Sheriff's Office
Gallatin County Sheriff's Office	Gallatin County Sheriff's Office
Glendive Police Department	Glasgow Police Department
Granite County Sheriff's Office	Great Falls Police Department
Great Falls Police Department	Helena Police Department
Havre Police Department	Hill County Sheriff's Office
Helena Police Department	Jefferson County Sheriff's Office
Jefferson County Sheriff's Office	Lake County Sheriff's Office
Lake County Sheriff's Office	Lewis & Clark County Sheriff's Office
Laurel Police Department	Lewistown Police Department
Lewis & Clark County Sheriff's Office	Lincoln County Sheriff's Office
Lewistown Police Department	Meagher County Sheriff's Office
Liberty County Sheriff's Office	Missoula Police Department
Livingston Police Department	Musselshell County Sheriff's Office
Madison County Sheriff's Office	Pondera County Sheriff's Office
Missoula Police Department	Powell County Sheriff's Office
Montana State University Police Department	Ravalli County Sheriff's Office
Park County Sheriff's Office	Sanders County Sheriff's Office
Petroleum County Sheriff's Office	Stillwater County Sheriff's Office
Pondera County Sheriff's Office	Thompson Falls Police Department
Sheridan County Sheriff's Office	Wheatland County Sheriff's Office
State Auditors Insurance Investigations	Whitefish Police Department
Teton County Sheriff's Office	
Thompson Falls Police Department	
Valley County Sheriff's Office	

APPENDIX 2

CICU Operating Costs FY 2023

OBPP Program	Org		Actuals Amount
05 DIV OF CRIMINAL INVESTIGATION			**704,467.02**
	0521 CIB Computer Crime Unit		**231,519.94**
		61000 Personal Services	202,192.88
		62000 Operating Expenses	16,609.94
		69000 Debt Service	12,717.12
	0521.1 DCI CIB Cybercrime		**731.99**
		61000 Personal Services	157.83
		62000 Operating Expenses	574.16
	0521.2 CIB ICAC		**187,549.61**
		61000 Personal Services	168,578.13
		62000 Operating Expenses	18,971.48
	05ICAC.21 DCI ICAC FFY21		**284,665.48**
		61000 Personal Services	86,980.35
		62000 Operating Expenses	144,423.04
		66000 Grants	53,262.09
Grand Total			**704,467.02**