Missouri Department of Public Safety
2023 State Cyber Crimes Grant (SCCG)
Notice of Funding Opportunity (NOFO)

Grant Issued By:

Missouri Department of Public Safety

Funding Opportunity Title

State Cyber Crimes Grant (SCCG)

Introduction

The goal of the SCCG Program is to make funds available to reduce internet sex crimes against children and improve public safety for children through investigations, forensics, and prevention. This program provides support of the continued operation of multi-jurisdictional law enforcement cybercrime task forces.

Funding Allocation

SCCG funds come from the Missouri General Revenue and are subject to request and approval each fiscal year.

Period of Performance: 12 months

Projected Period of Performance Start Date: June 1, 2022

Projected Period of Performance End Date: May 30, 2023

Funding Instrument: Grant

Eligible Applicants:

Any unit of state or local government within Missouri may apply for SCCG funds from the Missouri Department of Public Safety so long as the project is multi-jurisdictional. A Memorandum of Understanding (MOU) [or Memorandum of Agreement (MOA)], signed by all participating jurisdictions, must be submitted as an attachment to the application.

Ineligible Applicants

Non-profit and for-profit organizations are ineligible for SCCG funds from the State of Missouri.

Eligible Funding Areas

SCCG funds may be awarded for any one of the following budget categories as deemed necessary to effectively and efficiently operate the proposed project:

NOTE: Items must have a direct effect on combating and/or preventing cybercrimes, meaning that the item would be considered needed specifically to work such crimes. Flashlights, for example, may be used as an investigative tool during search warrants but are not deemed a tool specifically needed for investigating cybercrimes. This item should rather be provided by the officer's law enforcement agency. Costs will be considered for funding based on justification for each item and its direct relation to the purpose of this funding opportunity.

1. **Personnel, Personnel Benefits, Personnel Overtime, & Personnel Overtime Benefits**
   Salaries, overtime, and/or fringe benefits of detectives and forensic personnel whose focus is investigating internet sex crimes against children, including but not limited to, enticement of a child and possession or promotion of child pornography.

2. **Travel/Training**
   Training and travel-related costs of law enforcement and forensic personnel as well as prosecuting attorneys, circuit attorneys, and consultants hired to provide training at the project agency.

   Computer crime investigative/examination tasks generally fall into the following five (5) categories:

   1. Field Investigations
   2. Mobile Device Extractions
   3. Online Investigations
   4. Mobile Forensic Examinations
   5. Computer Forensic Examinations

   Cybercrime detectives and forensic personnel shall meet minimum training standards. The respective minimum training standards, by category, shall either be in place at the time of application, or the application shall include training scheduled within the grant period to address training needs.

   Police/Peace Officer Certification is mandatory and foundational in all aspects for Field Investigators and Online Investigators. Mobile Device Extractors, Mobile Forensic Examiners, and Computer Forensic Examiners may be certified officers or suitably trained civilian employees.

   Field Investigator

   Field Investigators are trained, equipped, and authorized to perform criminal investigations in the field. Field-level investigations are conducted by sworn officers with the power of search and seizure, as well as arrest powers. Field Investigators are viewed as the case agent and generally are tasked with overseeing the investigation from report through to adjudication (sometimes with assistance from other field investigators). In addition to those roles, duties of the Field Investigator include documenting complaints from reporting parties, victims, suspects, and witnesses through interviews and correspondence. Field Investigators also author and execute search warrants of physical locations and of requests for records stored online with internet service providers. The authoring of search warrants entails gathering information, compiling it, and obtaining necessary approvals from judges and prosecutors. Upon execution of search warrants, Field Investigators are authorized to seize, store, and obtain analysis of evidence in support of the investigation. Field Investigators are also empowered to arrest suspects. Lastly, Field Investigators compile the case

reports and other evidentiary items for presentation to the prosecuting authority and testify, as requested, through the trial process.

Minimum training:

- ☐ Police/Peace Officer Certification
- ☐ Training in the seizure of electronic evidence through one (or more) of the following courses:
  - Cellebrite's Cellebrite Mobile Forensic Fundamentals (CMFF)
  - FBI's ICAC Basic Course (through FBI's Computer Analysis Response Team/CART training)
  - ICAC/NCJTC's Seizing and Analyzing Mobile Devices
  - NDCAC's Gathering Evidence From Today's Communication Technologies
  - NW3C's CI-091 Introduction to Previewing
  - NW3C's DF-100 Basic Digital Forensic Analysis: Seizure (BDFA-Seizure)
  - NW3C's DF-101 Basic Digital Forensic Analysis: Windows Acquisition (BDFA-Win-Acq)
  - Other
- ☐ Training, and certification where certification is applicable, to utilize an on-scene tool through one (or more) of the following courses:
  - ADF Solutions' Digital Evidence Investigator (DEI)
  - FBI-RCFL's ImageScan
  - FBI's FTK Imager (through FBI's Computer Analysis Response Team/CART training)
  - ICAC/NCJTC's Introduction to osTriage
  - ICAC/NCJTC's osTriage Basic Investigations
  - Kroll's Kroll Artifact Parser and Extractor (KAPE)
  - Sumuri's Paladin
  - Other

Recommended training:

- ☐ Training in basic, entry-level, online investigations through one of the following courses:
  - ICAC/ NCJTC's Investigative Techniques (IT)
- ☐ If an officer is investigating Peer-to-Peer (P2P), on the job training by working with an experienced P2P investigator
  NOTE: Conducting field investigations of P2P cases is not the same as utilizing or running P2P software and thus has different expectations. An officer can conduct field investigations of P2P cases without formal training (although not recommended) but cannot obtain a P2P software license without training completion.

Mobile Device Extractor

Mobile Device Extractors are trained and authorized to utilize a cellular device kiosk station. (A kiosk is a preview tool that enables investigators to see a portion of the data quickly and easily; however, the kiosk was not designed to take the place of a full scale cell phone examination performed by a certified examiner.) This role can also include assisting or training other law enforcement officers to utilize a cellular device kiosk station.

Minimum training:

- ☐ Training from an experienced forensic examiner, or a fellow experienced mobile data extractor, on how to utilize a mobile data extractor tool

Online Investigator

Online Investigators are tasked with conducting investigations on the Internet. This role can include "chatting" (communicating) with suspects and victims in an undercover capacity in an effort to identify criminal conduct and gather evidence. This role may also include consulting law enforcement restricted databases, which document and track the distribution of child pornography, and developing leads for those investigations. In addition, this role may include monitoring and documenting advertisements, postings, social media, and any other publicly viewable online sources for leads to criminal conduct.

Minimum training:

- ☐ Police/Peace Officer Certification
- ☐ Training in basic, entry-level, online investigations through one (or more) of the following courses:
  - FBI's Online Covert Employee Course
  - ICAC/NCJTC's Investigative Techniques (IT)
  - Other
- ☐ Training in undercover communications through one (or more) of the following courses:
  - ICAC/NCJTC's Online Ads Investigations
  - ICAC/NCJTC's Undercover Chat (UC)
  - ICAC/NCJTC's Undercover Concepts and Techniques
  - Other
- ☐ If an officer is utilizing or running Peer-to-Peer (P2P) software, training on P2P investigations through one (or more) of the following software programs:
  - Ares
  - BitTorrent
  - eMule
  - ePhex
  - Freenet
  - Other

  NOTE: Utilizing or running P2P software is not the same as conducting field investigations of P2P cases and thus has different expectations. An officer cannot obtain a P2P software license without training completion but can conduct field investigations of P2P cases without formal training (although not recommended).

Recommended training:

- ☐ Eight or more hours annually of additional training in cybercrime investigations

Mobile Forensic Examiner

Mobile Forensic Examiners are investigators who are experts in gathering, recovering, analyzing and presenting data evidence from mobile devices using specialized forensic software and hardware. Mobile devices are defined in this context as cellular phones, tablets, cameras, and handheld GPS devices. This includes removable media used by those devices such as MicroSD cards. Forensics on mobile devices is an analysis of files beyond the attributes which are logically viewable by an ordinary user of the device. (Using forensic software or hardware to simply view and export

ordinarily viewable files and information is not restricted or limited to forensic examiners and can be performed by investigators.) Mobile Forensic Examiners are not required to be trained to the same level as Computer Forensic Examiners; the training may forego the basic computer knowledge and file system courses and can focus solely on mobile device forensics.

Minimum training:

- ☐ Training in basic, entry-level, mobile forensic examinations through one (or more) of the following courses:
  - Cellebrite's Certified Mobile Forensics Fundamentals (CMFF)
  - Cellebrite's Cellebrite Certified Operator (CCO)
  - DHS/FLETC's Mobile Device Investigations Program (MDIP)
  - FBI's Certified Forensic Examiner
  - ICAC/NCJTC's Seizing and Analyzing Mobile Devices
  - Magnet Forensics' AX100 Forensic Fundamentals
  - Magnet Forensics' AX200 Magnet AXIOM Examinations
  - MSAB's XRY Certification
  - NCFI's Mobile Device Examiner (MDE)
  - NCFI's Advanced Mobile Device Examiner (AMDE)
  - NDCAC's Collection/Seizure of Mobile Devices for Investigators
  - NW3C's DF-330 Advanced Digital Forensic Analysis: iOS & Android (ADFA-Mobile I)
  - PATC's Smartphone Forensics and Cellular Technology Certification (+SMART)
  - SANS' Smartphone Forensic Analysis In-Depth
  - SEARCH's Core Skills for the Investigation of Mobile Devices
  - Other
- ☐ Basic proficiency documentation or certification provided by a recognized trainer or authority through one (or more) of the following programs:
  - BlackBag Technology's Certified BlackLight Examiner (CBE)
  - BlackBag Technology's Certified Mobilyze Operator (CMO)
  - Cellebrite's Cellebrite Advanced Smartphone Analysis (CASA)
  - Cellebrite's Cellebrite Certified Mobile Examiner (CCME)
  - Cellebrite's Cellebrite Certified Operator (CCO)
  - Cellebrite's Cellebrite Certified Physical Analyst (CCPA)
  - FBI's Certified Mobile Device Examiner
  - IACIS' Certified Mobile Device Examiner (CMDE)
  - Magnet Forensics' AX200 AXIOM Examinations
  - Magnet Forensics' Magnet Certified Forensics Examiner (MCFE)
  - MSAB's XRY Certification
  - NCFI's Mobile Device Examiner (MDE)
  - SANS' GIAC Advanced Smartphone Forensics (GASF)
  - Other
- ☐ Vendor-specific training with one (or more) of the following forensic tools:
  - AXIOM (vendor: Magnet Forensics)
  - Cellebrite Inspector [formerly BlackLight] (vendor: Cellebrite)
  - Cellebrite UFED (vendor: Cellebrite)
  - EnCase Mobile Investigator (vendor: OpenText)
  - Oxygen (vendor: Oxygen Forensic)
  - Paraben (vendor: Paraben Corporation)
  - SecureView (vendor: SecureView)
  - XRY (vendor: MSAB)
  - Other

Recommended training:

- ☐ Eight or more hours annually of additional training in mobile forensic investigations

Computer Forensic Examiner

Computer Forensic Examiners are investigators who are experts in gathering, recovering, analyzing and presenting data evidence from computers and other digital media using specialized forensic software and hardware. Computer forensics is an analysis of files beyond the attributes which are logically viewable by an ordinary user of the device or media. (Using forensic software or hardware to simply view and export ordinarily viewable files and information is not restricted or limited to forensic examiners and can be performed by investigators.)

Minimum training:

- ☐ Training in basic, entry-level, computer forensic examinations through one (or more) of the following courses:
  - Cellebrite's Cellebrite Computer Forensic Fundamentals (CCFF)
  - Cellebrite's Cellebrite Apple Forensic Fundamentals (CAFF)
  - FBI's Certified Forensic Examiner
  - FLETC's Seized Computer Evidence Recovery Specialist (SCERS)
  - IACIS' Basic Computer Forensic Examiner (BCFE)
  - Magnet Forensics' AX100 Forensic Fundamentals
  - Magnet Forensics' AX200 Magnet AXIOM Examinations
  - NCFI's Basic Computer Evidence Recovery Training (BCERT)
  - NW3C's DF-103 Basic Digital Forensic Analysis: Windows Acquisition (BDFA-Win-Acq)
  - NW3C's DF-310 Advanced Digital Forensic Analysis: Windows (ADFA-Win)
  - NW3C's DF-320 Advanced Digital Forensic Analysis: macOS (ADFA-Mac)
  - Other
- ☐ Basic proficiency documentation or certification provided by a recognized trainer or authority through one (or more) of the following programs:
  - BlackBag Technology's Certified BlackLight Examiner (CBE)
  - Cellebrite's Cellebrite Computer Forensic Fundamentals (CCFF)
  - Exterro's [formerly AccessData] Certified Examiner (ACE)
  - Exterro's [formerly AccessData] Forensic Tool Kit (FTK) Bootcamp
  - FBI's Digital Extraction Technician (DEXT)
  - FLETC's Seized Computer Evidence Recovery Specialist (SCERS)
  - Griffeye's [formerly NetClean] Analyze Digital Investigator (DI) Certification
  - IACIS' Certified Forensic Computer Examiner (CFCE)
  - ISFCE's Certified Computer Examiner (CCE)
  - Magnet Forensics' AX200 AXIOM Examinations
  - Magnet Forensics' AX250 AXIOM Advanced Computer Forensics
  - Magnet Forensics' Magnet Certified Forensics Examiner (MCFE)
  - NCFI's Basic Computer Evidence Recovery Training (BCERT)
  - NCFI's Advanced Forensic Training (AFT)
  - NICCS' Certified Digital Forensics Examiner (CDFE)
  - NW3C's Certified Cyber Crime Examiner (CCCE) (3CE)
  - OpenText's EnCase Certified Examiner (EnCE)
  - Other

- ☐ Vendor-specific training with one (or more) of the following forensic tools:
  - AXIOM (vendor: Magnet Forensics)
  - Cellebrite Inspector [formerly BlackLight] (vendor: Cellebrite)
  - EnCase (vendor: OpenText)
  - Forensic Explorer (FEX) (vendor: GetData)
  - Forensic Tool Kit (FTK) (vendor: AccessData)
  - Griffeye Analyze [formerly NetClean] (vendor: Griffeye)
  - Paraben (vendor: Paraben Corporation)
  - X-Ways (vendor: X-Ways Software Technology AG)
  - Other _____

Recommended training:

- ☐ At least 8 hours annually of additional training in computer forensic investigations

3. **Equipment**
   Equipment is tangible, nonexpendable personal property (including information technology systems) having a useful life of more than one year and a per-unit acquisition cost of $1,000 or more per unit.

4. **Supplies/Operations**
   Supplies are all other items of tangible personal property that are not equipment. This includes technology and mobile devices that cost less than $1,000 per unit.

5. **Contractual**
   Costs directly associated with operating a cybercrime task force and its activities that are secured on a contractual nature.

I. Ineligible Activities and Cost Items:

Ineligible activities and cost items include, but are not necessarily limited to, the following:

- ❑ Bonuses or Commissions
- ❑ Construction/Renovation Projects
- ❑ Daily Subsistence within Official Domicile
- ❑ Entertainment Expenses & Bar Charges
- ❑ Finance Fees for delinquent payments
- ❑ First Class Travel
- ❑ Indirect Costs
- ❑ Less-than-lethal Weapons
- ❑ Lobbying or Fundraising
- ❑ Military-Type Equipment
- ❑ Office Lease/Purchase
- ❑ Personal Incentives for Employment
- ❑ Pre-Paid Fuel/Phone Cards
- ❑ Vehicles (Lease or Purchase)
- ❑ Weapons and Ammunition

Application and Submission Information

1. **Key Dates and Times**

   a. Application Start Date: March 21, 2022

   b. Application Submission Deadline: April 15, 2022 5:00 pm CST

2. **Agreeing to Terms and Conditions of the Award**

   By submitting an application, applicants agree to comply with the requirements of this NOFO and the terms and conditions of the award, should they receive an award.

   Applications will only be accepted through the Missouri Department of Public Safety (DPS) online WebGrants System. https://dpsgrants.dps.mo.gov/index.do

A PowerPoint with instructions on how to apply through the WebGrants System will be available on the DPS website, at the following link under 2023 State Cyber Crime Grant (SCCG) Program https://dps.mo.gov/dir/programs/cjle/sccg.php

As part of the SFY 2023 SCCG application, each eligible applicant must complete all application forms and provide all required documents:

1. **Contact Information Form**

2. **SCCG Project Package**

3. **Budget**

4. **Named Attachments**
   a. **Memorandum of Understanding (MOU), Memorandum of Agreement (MOA)**
   b. **Quote or Cost Basis**
   c. **Other Supporting Documentation**
   d. **Other Supporting Documentation**
   e. **Other Supporting Documentation**
   f. **Other Supporting Documentation**
   g. **Other Supporting Documentation**

Contact Information:

Additional information and resources can be located on the Missouri Department of Public Safety website: https://dps.mo.gov/dir/programs/cjle/sccg.php

WebGrants System, application submission site: https://dpsgrants.dps.mo.gov/index.do

Department of Public Safety Contacts:

Grant Specialist –
Becky Block
Rebecca.Block@dps.mo.gov
(573) 522-3455

Grants Program Supervisor –
Michelle Branson
Michelle.Branson@dps.mo.gov
(573) 526-9014

Program Manager –
Joni McCarter
Joni.McCarter@dps.mo.gov
(573) 526-9020