SFY 2027 State Cyber Crimes Grant (SCCG)

Notice of Funding Opportunity (NOFO)

Grant Issued By:

Missouri Department of Public Safety

Funding Opportunity Title:

SFY 2027 State Cyber Crimes Grant (SCCG)

Introduction:

The Missouri Department of Public Safety is pleased to announce the funding opportunity for the SFY 2027 State Cyber Crimes Grant (SCCG). These state administered funds are appropriated through Missouri House Bill No. 8 and are subject to request and approval each fiscal year.

Program Description:

The goal of the State Cyber Crimes Grant (SCCG) 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 for the continued operation of multi-jurisdictional law enforcement cybercrime task forces.

Period of Performance: 12 months

Projected Period of Performance Start Date: June 1, 2026

Projected Period of Performance End Date: May 31, 2027

Eligible Applicants:

Any unit of state or local government within Missouri may apply for SCCG funds from the Missouri Department of Public Safety so as 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:

- ☐ Nonprofit organizations
- ☐ For-profit organizations
- ☐ Agencies applying for a project that does not support a multi-jurisdictional task force

DPS GRANTS – STATE REQUIREMENTS

To be eligible for grant funding through the Missouri Department of Public Safety (DPS), agencies must be compliant with the requirements listed below (as applicable) at the time of application and if awarded funding, must maintain compliance throughout the grant period of performance.

LAW ENFORCEMENT REQUIREMENTS

These requirements below apply only to law enforcement agencies.
Each law enforcement agency shall certify compliance with these requirements below when applying for grants administered by the DPS.

Section 590.650 RSMo – Vehicle Stops Report

Pursuant to Section 590.650.3 RSMo, each law enforcement agency shall compile the data described in subsection 2 for the calendar year into a report to the attorney general and each law enforcement agency shall submit the report to the attorney general no later than March first of the following calendar year.

NOTE: Failure to submit the Vehicle Stops (Racial Profiling) Report will result in the automatic denial of the application.

Section 590.700 RSMo – Written Policy on Recording of Custodial Interrogations

Pursuant to Section 590.700.4 RSMo, each law enforcement agency shall adopt a written policy to record custodial interrogations of persons suspected of committing or attempting to commit felony crimes as outlined in subsection 2.

Section 43.544 RSMo – Written Policy on Forwarding Intoxication-Related Traffic Offenses

Pursuant to Section 43.544.1 RSMo, each law enforcement agency shall adopt a policy requiring arrest information for all intoxication-related traffic offenses be forwarded to the central repository as required by Section 43.503 RSMo.

Section 590.1265 RSMo – Police Use of Force Transparency Act of 2021

Pursuant to Section 590.1265 RSMo, each law enforcement agency shall report data submitted under subsection 3 of this section to the department of public safety.

For purposes of grant eligibility, law enforcement agencies will be considered non-compliant if they have not submitted Use of Force reports for three or more months in the previous 12 months.

NOTE: Show Me Crime Reporting provides a no cost option for agencies to comply with Section 590.1265 RSMo. Agencies not currently compliant with Section 590.1265 RSMo will not be eligible to apply until they have registered with Show Me Crime Reporting and have begun submitting Use of Force reports.
https://showmecrime.mo.gov/CrimeReporting/ForcePage.html

Section 43.505 RSMo – Uniform Crime Reporting (UCR)

Pursuant to Section RSMo 43.505.3, each law enforcement agency in the state shall: (1) Submit crime incident reports to the department of public safety on forms or in the format prescribed by the department; and (2) Submit any other crime incident information which may be required by the department of public safety.

Agencies not compliant at the time of application will be ineligible for funding.

For purposes of grant eligibility, law enforcement agencies will be considered non-compliant if they have not submitted MIBRS reports for three or more months in the previous 12 months.

NOTE: Show Me Crime Reporting provides a no cost option for agencies to comply with Section 43.505 RSMo. Agencies not currently compliant with Section 43.505 RSMo will not be eligible to apply until they have registered with Show Me Crime Reporting and have begun submitting MIBRS reports.
https://showmecrime.mo.gov/CrimeReporting/MIBRSRegistration.html

Section 590.030 RSMo – Rap Back Program Participation

Pursuant to Section 590.030 RSMo, all law enforcement agencies shall enroll in the state and federal Rap Back programs on or before January 1, 2022 and continue to remain enrolled. The law enforcement agency shall take all necessary steps to maintain officer enrollment for all officers commissioned with that agency in the Rap Back programs. An officer shall submit to being fingerprinted at any law enforcement agency upon commissioning and for as long as the officer is commissioned with that agency.

Allowable Costs:

Requested item(s) must have a direct effect on combating and/or preventing cybercrimes, meaning that the item(s) would be 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.

Applicants may request funding under the approved budget categories listed below to support multi-jurisdictional law enforcement cybercrime task forces:

- ☐ **Personnel/Personnel Overtime**
  Salaries and/or overtime 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.

- ☐ **Personnel Benefits/Personnel Overtime Benefits**
  Fringe benefits and/or overtime 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.

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

  Please reference Appendix A for training standards of cybercrime detectives and forensic personnel.

- ☐ **Equipment**
  Equipment is tangible property having an acquisition cost of $5,000 or more per unit and a useful life of more than one year.

- ☐ **Supplies/Operations**
  Supplies are defined as property with an acquisition cost of less than $5,000 per unit or a useful life of less than one year. Operations are defined as operational costs necessary to perform project activities, such as rent and phone expenses for example.

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

Unallowable Costs:

Unallowable costs include, but are not limited to, the following:

- ☐ Bonuses or Commissions
- ☐ Construction/Renovation Projects
- ☐ Daily Subsistence within Official Domicile
- ☐ Entertainment Expenses and 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. **Applications will only be accepted through the Missouri Department of Public Safety (DPS) online WebGrants System:** Department of Public Safety DPS Grants (mo.gov)

2. **Key Dates and Times**
   a. **Application Start Date:** May 4, 2026
   b. **Application Submission Deadline:** June 1, 2026, 5:00 pm CST

3. **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.

   A PowerPoint with instructions on how to apply through the WebGrants System will be available on the Missouri Department of Public Safety website, at the following link: https://dps.mo.gov/dir/programs/dpsgrants/sccg.php.

   As part of this application, each eligible applicant must complete all application forms and provide all required documents:

   1. **Contact Information Form**

   2. **DPS Grants State Requirements**

   3. **Project Package**

   4. **Budget**

   5. **Named Attachments**
      a. **Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA)**
      b. **Quote/Cost Basis**
      c. **Other Supporting Information (up to 5 attachments)**

Department of Public Safety Contacts:

Sandy Kremer
Grants Specialist
(573) 751-5997
Sandy.Kremer@dps.mo.gov

Amelia Jaegers
Lead Grants Specialist
(573) 522-4094

Amelia.Jaegers@dps.mo.gov

Chelsey Call
Grants Supervisor
(573) 526-9203
Chelsey.Call@dps.mo.gov

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

Kelsey Saunders
Grant Support Specialist
(573) 522-6125
Kelsey.Saunders@dps.mo.gov

Appendix A

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

The positions associated with these computer crime investigative/examination tasks are described below:

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.

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.

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 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.

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.

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.

Training Standards:

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 the training requirements.

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.

The table below demonstrates the minimum required training as well as recommended training for each of the positions discussed above.

Position Type	Minimum Training	Recommended Training
Field Investigator	▪ Police/Peace Officer Certification ▪ Training in the seizure of electronic evidence through one (or more) of the following courses:	▪ Training in basic, entry-level, online investigations

	▪ 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 are 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	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 difference 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	▪ Training from an experienced forensic examiner, or a fellow experienced mobile data extractor, on how to utilize a mobile data extractor tool	
Online Investigator	▪ 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) ▪ Basic ICAC Investigations (MO ICAC) ▪ Other	▪ Eight or more hours annually of additional training in cybercrime investigations

	▪ 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)	

Mobile Forensic Examiner	▪ 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)
		▪ Eight or more hours annually of additional training in mobile forensic investigations

	▪ 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 ▪ 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 (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	
Computer Forensic Examiner	▪ 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 Certified Examiner ▪ Exterro's Forensic Tool Kit (FTK) Bootcamp	▪ At least eight hours annually of additional training in computer forensic investigations

	▪ FBI's Digital Extraction Technician (DEXT)
	▪ FLETC's Seized Computer Evidence Recovery Specialist (SCERS)
	▪ Griffeye's 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)
	▪ 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 (vendor: Cellebrite)
	  ▪ EnCase (vendor: OpenText)
	  ▪ Forensic Explorer (FEX) (vendor: GetData)
	  ▪ Forensic Tool Kit (FTK) (vendor: AccessData)
	  ▪ Griffeye Analyze (vendor: Griffeye)
	  ▪ Paraben (vendor: Paraben Corporation)
	  ▪ X-Ways (vendor: X-Ways Software Technology AG)
	  ▪ Other	