Local Law Enforcement Grants for the Enforcement of Cybercrimes

FY 2024 Pre-Application Session February 15, 2024



Introductions and Goals

- Elaina Roberts, Grant Management Specialist
- Krista Blakeney-Mitchell, Associate Director
- Sheila Griese, Management Analyst
- Goals:
 - Focus on key aspects of the Cybercrimes Enforcement Program solicitation.
 - Provide relevant information and answers to your questions.

Applicants are responsible for reading the solicitation and solicitation companion guide.





- About the Cybercrimes Enforcement Program
- Important deadlines and eligibility requirements
- Program requirements and out-of-scope activities
- How to apply
- Resource for applicants





The Office on Violence Against Women





The Office on Violence Against Women (OVW) provides federal leadership in developing the national capacity to reduce violence against women and administer justice for and strengthen services to victims of domestic violence, dating violence, sexual assault, and stalking.



Learn more about our grants at: Justice.gov/OVW/Grant-Programs





About the Cybercrimes Enforcement Program





About the Program

- Passed in the Violence Against Women Act Reauthorization Act 2022 and is codified in 34 U.S.C. § 30107.
- The Cybercrimes Enforcement Program (CFDA # 16.060) supports efforts by States, Indian Tribes, and units of local government to prevent, enforce, and prosecute cybercrimes against individuals.
- Includes training for law enforcement, prosecutors, judges and judicial personnel on cybercrimes as well as assistance to agencies enforcing laws, educating the public, supporting victim assistants, establishing task forces, and acquiring computers and equipment to conduct investigations and forensic analysis of evidence.





Cybercrimes Definition

- Cybercrimes against individuals are defined as criminal offenses that involve the use of a computer to harass, threaten, stalk, extort, coerce, cause fear to, or intimidate an individual, or without consent distribute intimate images of an adult, except that use of a computer need not be an element of the offense. (See 34 U.S.C. § 30107(a)(2)).
- The term computer includes a computer network and an interactive electronic device.
- Cybercrimes against individuals *do not* include the use of a computer to cause harm to a commercial entity, government agency or nonnatural person.





Program Award Information

- Grant award period is 36 months.
- OVW anticipates the award period will start October 1, 2024.
- Projects can receive up to \$500,000 for the 36-month period.
- OVW anticipates funding ten projects for a total of \$5,000,000.



OVW Priority

- In FY 24 OVW has four programmatic priorities.
- Priority 1, Advancing equity and tribal sovereignty as essential components of ending sexual assault, domestic violence, dating violence, and stalking applies to this program.
- Applicants are encouraged but not required to address this priority area. (see pages 7 8 for detailed information).





Important Deadlines and Eligibility Requirements





Application Deadlines

- Application submissions are due by 8:59 PM Eastern Time on May 1, 2024.
- Application submitted through a <u>two-step process</u>:
 - Submission of SF-424 and SF-LLL in Grants.gov by April 29, 2024, at 11:59 PM ET.
 - Submission of the full application including all attachments in the Justice Grants System (JustGrants) by May 1, 2024, at 8:59 PM ET.





- Eligible applicants are limited to: States, Indian Tribes, and units of local government. (see page 10)
- Note: agencies of units of local government are not eligible to *apply* but they can be the recipients of the funding.
- All applicants are new. This is the first year of funding.



Certifications and Assurances Letter

- All applicants must submit a certifications and assurances letter.
- Certifications must take the form of a letter, on letterhead, signed, and dated by the authorized representative (for this program, the authorized representative is the chief executive officer of a state, Tribal government, or unit of local government).
- A sample letter is linked on page 12 of the solicitation.
- OVW encourages using the sample letter.



Certifications and Assurances (slide 1)

Federal funds made available under the Local Law Enforcement Grants for Enforcement of Cybercrimes Program will not be used to supplant State, Tribal, or local funds, but will be used to increase the amounts of such funds that would, in the absence of Federal funds, be made available for law enforcement activities;

(i) the programs to be funded by the grant meet all the requirements of 34 U.S.C. § 30107;
(ii) all the information contained in the application is correct;
(iii) there has been appropriate coordination with affected agencies; and

(iv) the applicant will comply with all provisions of 34 U.S.C. § 30107 and all other applicable Federal laws;



Certifications and Assurances (slide 2)

the [State, Tribe, or in the case of a unit of local government, the State in which the unit of local government is located,] has in effect criminal laws which prohibit cybercrimes against individuals;

any equipment described in purpose area 34 U.S.C. § 30107 (d)(8) purchased using grant funds <u>awarded</u> under the Local Law Enforcement Grants for Enforcement of Cybercrimes Program will be used primarily for investigations and forensic analysis of evidence in matters involving cybercrimes against individuals.





Certifications and Assurances (slide 3)

not later than 30 days before the application (or any amendment to the application) was submitted, the application (or amendment) was submitted for review to the governing body of the State, Tribe, or unit of local government (or to an organization designated by that governing body);

before the application (or any amendment to the application) was submitted the application (or amendment) was made public and an opportunity to comment on the application (or amendment) was provided to citizens, to neighborhood or community-based organizations, and to victim service providers, to the extent applicable law or established procedure makes such an opportunity available;

for each fiscal year covered by an application, the applicant shall maintain and report such data, records, and information (programmatic and financial) as the Attorney General may reasonably require.



Program Requirements and Out-of-Scope Activities







- There are ten statutory purpose areas for this program (see pages 6 7).
- Applicants are **required** to address **purpose area 1 and/or 2**.
- Applicants may choose to address additional purpose areas.
- There is no limit to the number of purpose areas addressed.





- Training for State, Tribal, or local law enforcement personnel relating to cybercrimes against individuals. (see page 6)
- Includes six topics relate to this purpose area (A F on page 6 of the solicitation).
- Focus must be on comprehensive training for law enforcement personnel.





- Training for State, Tribal, or local prosecutors, judges, and judicial personnel relating to cybercrimes against individuals. (see page 6)
- Includes four topics that relate to this purpose area (A D on page 6 of the solicitation).
- Focus must be on comprehensive training for prosecutors, judges, and judicial personnel.





- If applicants choose to apply for purpose area 8, acquiring computers, computer equipment, and other equipment, please note the funds for the acquisition of this equipment cannot exceed 50% of the total budget. This means that for a \$500,000 budget, no more than \$250,000 can go towards the purchase of the equipment.
- The equipment must primarily be used for the investigation and forensic analysis of cybercrimes against individuals.



Required Partnership

Every applicant is required to partner with a victim service provider. (see page 12)

A victim service provider is a nonprofit, nongovernmental or tribal organization or rape crisis center, including a State or tribal domestic violence and/or sexual assault coalition, that assists or advocates for domestic violence, dating violence, sexual assault, or stalking victims, including a domestic violence shelter, faith-based organization or other organization, with a documented history of effective work concerning domestic violence, dating violence, sexual assault, or stalking. See 34 U.S.C. § 12291(a)(50). Victim service providers must provide direct services to victims of domestic violence, dating violence, sexual assault, or stalking as one of their primary purposes and have a demonstrated history of effective work in this field.

The partnership must be documented in the Memorandum of Understanding. (pages 19 – 20)



Program Requirements

- Applicants that receive funding must (among other activities listed):
 - Establish or continue a coordinated community response (CCR) team.
 - Address the intersection of gender-based violence and cybercrimes against individuals.
 - Implement **purpose area 1 and/or 2** (also an application requirement).
 - Partner with a victim service provider (also an application requirement).
 (See pages 9 10 for more details)



Out-of-Scope Activities

- Funds may not be used for:
 - Research projects.
 - Activities related to the distribution of intimate images of a minor.
 - Cybercrime related to the use of a computer to cause harm to a commercial entity, government agency, or nonnatural person.

(See page 8 of the solicitation)



How to Apply





How to Apply (continued)

- Applicants may find this funding opportunity on **Grants.gov** by using the Assistance Listing number (16.060), Grants.gov opportunity number (O-OVW-2024-171924), or the title of the solicitation.
- Application process requires two-steps:
 - Application will be started in Grants.gov (SF-424 and SF-LLL).
 - Application will continue and be submitted in JustGrants.



Getting from Grants.gov to JustGrants

 After submitting the two forms in Grants.gov the applicant will receive an email notification from JustGrants to complete the rest of the application in JustGrants. If the applicant is a new user in JustGrants, the email will include instructions on registering with JustGrants.





JustGrants: Application Documents

- Proposal Narrative (purpose, what will be done, who will implement).
- Budget and Budget Narrative
- Memorandum of Understanding (MOU)
- Certifications and Assurances Letter



JustGrants: Application Documents, Other

- Proposal Abstract entered into a text box in JustGrants.
- Data Requested With Application:
 - Pre-Award Risk Assessment
 - Applicant Entity Questionnaire
 - Summary Data Sheet



Grants Financial Management Division

Pre-Award Risk Assessment, online questionnaire

- Eleven questions; Multiple parts to each question.
- Most common issues:
 - Brief list of policies and procedures not provided;
 - Budgeted vs. Actual process not provided;
 - Record Retention policy not provided;
 - Lack of knowledge of federal rules and regulations.



Where to Begin

- Read the solicitation carefully to understand all steps required to submit an application and the time to complete those steps.
- Some steps, such as obtaining a Unique Entity Identifier (or UEI) number or registering with the System for Award Management (SAM) or Grants.gov may take several days to complete.
- We recommend applicants begin these processes as soon as possible but no later than dates suggested in the solicitation.



Resources for Applicants





DOJ Application Resources

- Open OVW Program Solicitations: Office on Violence Against Women (OVW) | Open Solicitations (justice.gov)
- The Department of Justice has made a collection of self-guided training resources, including training and a Virtual Q&A session on Application Submission, available at:

https://justicegrants.usdoj.gov/trainingresources/justgrants-training/grants-managementlifecycle



Financial Resources

- Budget Information and Sample Budget Detail Worksheet: <u>https://www.justice.gov/ovw/page/file/1107316/download</u>
- Creating a Budget: <u>https://www.justice.gov/ovw/video/creating-budget</u>
- Uniform Guidance 2 CFR Part 200: <u>https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200?toc=1</u>
- DOJ Financial Guide: <u>https://www.justice.gov/media/1282146/dl?inline=</u>



Helpful Contacts

- Programmatic Questions: OVW.cybercrimes@usdoj.gov or call 202-307-6026
- Financial Questions: OVW.GFMD@usdoj.gov or call 1-888-514-8556
- Technical Questions:
 - Grants.gov Applicant Support: support@grants.gov or call 800- 518-4726
 - OVW JustGrants Support: OVW.JustGrantsSupport@usdoj.gov or call 866-655-4482







