FY2024 Local Law Enforcement Grants for the Enforcement of Cybercrimes Pre-Application Information Session

February 15, 2024

ELAINA ROBERTS: Good afternoon, everyone. Thank you for joining us for the Fiscal Year 2024 Local Law Enforcement Grants for the Enforcement of Cybercrimes program, referred to as the Cybercrimes Enforcement Program pre-application session. This session is for the FY 24 solicitation that was posted on January 31st. My name is Elaina Roberts, and I am the grant management specialist for the Cybercrimes Enforcement Program. I am joined by Associate Director Krista Blakeney-Mitchell, who oversees the cybercrimes program, as well as the Rural and Consolidated Youth programs. Also on this call is Sheila Griese, a Management Analyst at OVW.

Our goals for this session include focusing on key aspects of the Cybercrimes Enforcement Program solicitation and providing relevant information and answers to your questions. This is not intended to be a comprehensive review of the solicitation and applicants are expected to fully read the solicitation before applying. That said, this is a new program, and you may have lots of questions, which we welcome. In the interest of time, I am asking that you hold all of your questions until the end. If you cannot stay for the entire session, please drop your questions into the Q&A box along with your email, if you feel comfortable, and I will respond to you. You may also email the ovw.cybercrimes@usdoj.gov email box. Finally, if you don't already have the solicitation in front of you, this may be a good time to get it out, as I will be referencing certain parts of it along with the page numbers. In today's session, we will provide you with information about the Cybercrimes Enforcement Program, provide important deadlines and eligibility requirements, go over the program requirements and out-of-scope activities under the program, and finally, we'll go over the two-step application process that is required of all applicants. At the end of the slides are resources and contact information to assist you as you begin your applications. Many of you already know, but just in case, this program is administered by the Office on Violence Against Women, or OVW. 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.

Let's first start by going over what this program is all about. The Cybercrimes Enforcement Program was passed in the recent reauthorization of the Violence Against Women Act or VAWA, V-A-W-A, 2022. It is codified in 34 U.S.C., Section 30107. The program supports efforts by states, Indian Tribes, and units of local government to prevent, enforce, and prosecute cybercrimes against individuals. It includes training for law enforcement, prosecutors, judges, and judicial personnel on cybercrimes against

individuals, as well as provides assistance to agencies to enforce laws, educate the public, support victim assistance, establish task forces, and acquire computers and equipment to conduct investigations and forensic analysis of evidence of cybercrimes against individuals.
Next, we'll look at the definition of cybercrimes against individuals. 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 the use of a computer need not be an element of the offense. 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, a government agency, or a non-natural person. In other words, this program is not intended to investigate or prosecute cybercrimes against corporations, entities, or even your own agency. Often in the news we hear about breaches or companies being hacked and information stolen. This is not what this program is for. It must be a cybercrime against a person. This does include crimes, such as cyberstalking, cyber harassment, and a non-consensual distribution of an intimate image.

Awards made under this program will be for 36 months. OVW anticipates the award period starting on October 1st, 2024. And projects can receive up to 500,000 for the entire 36-month period. We anticipate funding for up to 10 projects for a total of 5 million. Finally, this program has an OVW priority in the solicitation. In FY 24, OVW has four programmatic priorities. This program has chosen to apply priority one, advancing equity and Tribal Sovereignty as essential components of ending sexual assault, domestic violence, dating violence, and stalking. While applicants are encouraged to address this priority in their applications and projects, it is not a requirement. Applicants who choose to address it may receive special consideration for their application. Please see pages seven through eight for what is necessary to meet this priority.

Let's turn to the very important deadlines and eligibility requirements. Some good news for applicants – and thank you to those of you who wrote in to notify us of the tight turnaround originally in the solicitation – we have extended the deadline to submit applications. Applications are now due by 8:59 PM Eastern Time on May 1st, 2024. The original deadline of March 21st does not apply anymore. The new deadline is May 1st. Submitting an application is a two-step process over the course of several days. You will first submit the SF-424, which is the application for federal assistance, and the SF-LLL disclosure of lobbying activities form in Grants.gov. You must submit these forms in Grants.gov by April 29th at 11:59 PM Eastern. Otherwise, you will not be able to then submit your full application in the Justice Grants system known as JustGrants by 8:59 PM on May 1st. This is two days after the Grants.gov deadline. I have highlighted the

8:59 PM Eastern deadline time because this is new over the last several years. Please note that this is not a midnight deadline. We'll go over this process in more detail at the end of this session.

Eligible applicants for this program are limited to states, Indian Tribes, and units of local government. Please note that agencies of units of local governments such as police departments, district attorney's offices, probation or parole offices, and any agency within a local government, are not eligible applicants. However, even though the agency themselves cannot apply for the funding, they can be the recipients of the funding. As I stated, this is a new program this year, so all applicants will be new. Please see page 10 of the solicitation for more information.

All applicants must submit a Certifications and Assurances Letter with their application. 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. It will be uploaded as an attachment in JustGrants. There is a sample letter that is linked on page 12 of the solicitation and applicants are encouraged to use that sample letter when completing their applications. I will highlight just a few aspects of the Certifications and Assurances Letter. First, applicants must certify that funds under this program will not be used to supplant state, Tribal, or local funds. This is important to note that you are asked to certify this in the letter. This means there is not a separate letter of non-supplanting that is required under this program. Second, you must certify that you already have in effect criminal laws that prohibit cybercrimes against individuals. Again, this may be statutes related to cyberstalking, cyber harassment, and the non-consensual distribution of intimate images, among others. Remember, the statutes must relate to cybercrimes against individuals and not non-natural entities. Finally, for applicants who choose to purchase equipment under this program, you must certify that the equipment will be used primarily for the investigation and forensic analysis of evidence in matters involving cybercrimes against individuals. Every applicant will certify this even if they are not currently proposing the purchase of equipment in the application.

There are several assurances in the letter as well. I'm just going to cover the first two. First, applicants must assure that not later than 30 days before the application was submitted, it was submitted for review to the governing body of the state, Tribe, or unit of local government. This is likely a process most of you already have in place, but I just want to point out that this assurance says nothing about receiving the final approval before you can submit your application, only that you must submit for review at least 30 days before you actually submit the application. Also, before the application was

submitted, applicants must assure that the application was made public and an opportunity to comment was provided. To the extent, applicable law or established procedure makes such an opportunity available. You may not have any requirement under your laws or regulations to do this. If you don't, then you can still assure that you complied with this assurance. Now, let's turn to the program requirements and out-of-scope activities.

This program has 10 statutory purpose areas that applicants can address. However, please note that applicants are required to address Purpose Area 1 or Purpose Area 2. These relate to training for law enforcement, prosecutors, judges, and judicial personnel that we'll go over in more detail in just a moment. Applications received that do not address either one of these purpose areas will not be considered for funding. Every applicant must address Purpose Area 1 or Purpose Area 2, or you can do both. Once you have this, you may address any of the other purpose areas listed in the solicitation. There is no limit to how many purpose areas you can address. Let's go over each one in greater detail.

Purpose Area 1 is training for state, Tribal, or local law enforcement personnel relating to cybercrimes against individuals. Under this purpose area are six topics that relate to comprehensive training for law enforcement personnel. Please see page six of the solicitation. Several people have written in to ask about the types of trainings and if they are required to develop them themselves. You'll see when we get to the required partnerships that we require each applicant to partner with a victim service provider. OVW believes in these partnerships to provide wraparound holistic services to victims and also to help coordinate communication with the victims to provide a trauma-informed lens from which the criminal justice and allied professionals can work from. It is expected that applicants who are funded work with their victim service provider partner to develop or deliver comprehensive training for their community. You may also use funds to attend other trainings that focus on cybercrimes against individuals. However, developing and using the training versus sending law enforcement to a conference will allow each officer the opportunity to receive that training. Finally, if there is a training that exists and you're able to take it and use it and use the applicable parts, that would be fine, too. For instance, trainings regarding conducting forensic analysis of different operating systems can usually be applied across the board. However, as everyone on this call knows, laws differ from state to state so what applies or works in one state may not work in another. It is important to tailor the training to your applicable laws.

Purpose Area 2 is training for state, Tribal, or local prosecutors, judges, and judicial personnel relating to cybercrimes against individuals. This purpose area includes four

topics. Again, the focus must always be on providing comprehensive training for prosecutors, judges, and judicial personnel on cybercrimes against individuals. What I stated just a moment ago regarding the development of the training holds true for this purpose area as well. Every applicant will have to partner with a victim service provider. This partnership can help serve victims better and help in the development of robust, statute-specific cybercrimes training.

Purpose Area 8, the acquisition of equipment is not a required purpose area. But I want to note here that for applicants that choose to address this purpose area, no more than 50% of the funds can go toward the purchase of the equipment. This means that for a $500,000 budget, no more than $250,000 can go toward the purchase of equipment. As I mentioned, every applicant is required to partner with a victim service provider. A victim service provider is a non-profit, non-governmental, 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.

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. It is critical that this partnership be brought into the fold of the project and is not just a listed partner who has no input or responsibilities under the project. Applicants should refer to the What Will be Done and Who Will Implement sections on pages 15 through 17 of the solicitation and respond directly to the call of each number under that section. Additionally, and this is critical, the partnership must be documented in the Memorandum of Understanding, the MOU, and be signed by both parties. Failure to submit a signed MOU with the application will result in removal from further consideration. Please refer to pages 19 through 20 of the solicitation.

Applicants that receive funding must engage in the following, among other activities listed -- establish or continue a coordinated community response or CCR team. This must be done within the first six months of the award. The CCR team must focus on cybercrimes against individuals. It should not be a team focused on general crime or even on any of the VAWA crimes. There must be a focus on the crimes that are occurring and that the laws in your state address. Additionally, a cornerstone of this program is the intersection of gender-based violence and cybercrimes or attack-facilitated abuse. We know that women and girls and LGBTQ+ individuals experience higher rates of violence including online abuse. Applicants should not only address this

intersection in the application but must also address this in their projects if funded. We've already gone over the last two program requirements, so I will not do that again here.

Finally, the following are out-of-scope activities and will not be supported by this program, research projects, activities related to the distribution of intimate images of a minor, which I will come back to, and cybercrimes related to harm to a commercial entity, government agency, or non-natural person. The authorizing statute for this program is clear, that only the non-consensual distribution of intimate images of an adult is authorized. This is not a program that will focus on intimate images of minors or child sexual abuse material referred to as CSAM, C-S-A-M. Next, I will cover how to apply. Applicants may find this funding opportunity on Grants.gov by using the Assistance Listing number, 16.060, and the Grants.gov opportunity number, 0-OVW-2024-171924. And I misspoke, it starts with an O, not a zero, so I apologize. It's O-OVW. Or the title of the solicitation.

The application process requires two steps. First, you will start the application in Grants.gov. This is where you will upload the filled-out SF-424 and SF-LLL documents. Second, the application process will continue and be submitted in JustGrants. Now, you might be wondering, “How do you get from Grants.gov to the JustGrants system so that you can finish?” And I'll go over that now. After an applicant submits the two forms in Grants.gov, the applicant that is registered will receive an email within 24 hours from JustGrants, prompting them to complete the rest of the application. This is when the applicant will upload all the other required documents. If the applicant is new to the system and has never applied in JustGrants before, the email will prompt the user to register with JustGrants and establish an entity administrator. The entity administrator is responsible for managing entity-level information and assigning the various roles in a JustGrants system. This person is also the E-Biz -- and that's B-I-Z -- point of contact designated in the SAM.gov system, S-A-M, .gov system, where grantees have access to their funds. We did not go over SAM.gov today, but please note applicants must register and be able to access each of the systems described in the solicitation. Registering can take several weeks altogether, so please start the process today.

Once applicants log in to the JustGrants system to finish and submit the application, which is the Proposal Narrative, the Budget and Budget Narrative, the MOU, and the Certifications and Assurances Letter, these will be uploaded as attachments and there will be online questionnaires to complete, such as the Pre-Award Risk Assessment, the Applicant Questionnaire, and the Summary Data Sheet. Please note that you will be prompted to add a Proposal Abstract in a text box. The Abstract is not scored but helps us to have an overview of the proposed project. The Data Requested with Application

includes three online questionnaires, the Pre-Award Risk Assessment, the Applicant Entity Questionnaire, and the Summary Data Sheet. Every applicant must fill it out with the application. The questionnaires are reviewed by OVW's Grants Financial Management Division or GFMD team.

I'm going to touch first on the Summary Data Sheet. There is a question regarding whether the applicant has expended $750,000 or more in federal funds during their last fiscal year. If yes, then the applicant must provide the end date of their last fiscal year. GFMD frequently finds that applicants do not include the date in their information, so please do be sure to do this if it applies to you. The next questionnaire I want to touch on is the Pre-Award Risk Assessment. GFMD has found in prior years that applicants do not fully answer all parts of the questions. This requires GFMD to reach out to the applicant, which may delay funding decisions. Common issues encountered include applicants who indicate they have internal policies in place but then do not provide the specific list of topics covered in those policies and procedures. Also, applicants may fail to provide the process for tracking expenditures and, more specifically, whether or not they are tracking budgeted versus actual expenditures. These are just a few examples. Please be sure to read and respond to each part of the question.

So, where to begin? First, read and probably re-read through the solicitation to understand all the steps that are required to submit an application. You should anticipate that those steps will take several days and up to a few weeks to fully complete. I am referring to everything outside of writing the application, though that will take time, too. But I cannot emphasize enough that some steps, such as obtaining a Unique Entity Identifier or UEI for folks who have never applied for a DOJ grant before or registering with SAM.gov and Grants.gov will each take several days to complete. Every year, we hear from folks who underestimate the amount of time setting up these systems takes. We recommend starting the process now, but for sure no later than the dates listed in the solicitation. Do not wait to do this. You will run out of time. Finally, please remember that you must begin the submission process in Grants.gov by April 29th. This is two days prior to the application deadline in JustGrants on May 1st at 8:59 PM Eastern. Those of you in earlier time zones, please note that this is an Eastern Time. So, please plan accordingly so you don't miss the deadline.

Lastly, I want to provide you with some helpful resources as you go through the application process. You can find all open OVW solicitations, including the cybercrimes enforcement one, on the OVW site. Please look under the “Funding” tab, then click “Open Solicitations.” Also, the Department of Justice has made a collection of self-guided training resources, including training and a virtual Q&A session on application submission. It's available under the justicegrants.usdoj.gov site. I will drop this link into

the chat now. Please bookmark it on your web browser. There are also several financial resources available to applicants. These can assist in budget development and provide other federal financial guidance. I want to highlight the Creating a Budget bullet point. This is a webinar by GFMD on how to develop a budget. Also listed are the Uniform Guidance found at 2 CFR 200 and the DOJ Financial Guide. And, of course, you can always reach out to us at OVW if you have any questions with the submission of your applications. Please note that we cannot comment on or provide insight into your proposed project, but we are here to assist with technical or confusing processes.

And with that, I will open it up for questions. I'm going to leave this last slide up, just in case. "Does this program apply to minors or juveniles? Many law enforcement agencies have internet crime against children, or ICAC units, who are interested in applying." It does, and it doesn't. It doesn't apply specifically to crimes against children. It applies to cybercrimes against individuals. And, again, one of the unallowable activities is the focus on the non-consensual distribution of intimate images of minors.

I have another question. "I'm with a county prosecutor's office. However, when we apply for grants, can we apply as the county of Macomb?" The answer is yes. Counties are eligible. It's the agency within the unit of local government. So, again, a prosecutor's office or police law enforcement office. The offices themselves, those agencies are not eligible to apply. But counties, parishes, cities -- all those units of local government are eligible. The rest of the question asks, "Can we include the sheriff's department under the same application?" And I'm not exactly sure what you mean by "can we include." Again, any agency of a unit of local government can be a recipient of the funds. They just can't be the ones applying for the funds. If that is not clear, please raise your hand or write in again, but I'll keep going.

So, it says, "To be clear, for a city, the mayor's office or public health or human services can apply but not the police?" What I can tell you is that the statute says it must be a unit of local government. And so, if the mayor's office represents the city and they are the chief executive officer, then yes, they can apply. So, it would come most likely from that agency--from that unit of local government. I don't know enough about public health or human services to know how that's structured, so I don't think I can answer the rest of that question. But maybe if you could write into the OVW.cybercrimes email, we can chat more online.

"Can you please explain more about the unit of local government? For example, can a city lead,"— so, yes. I think I answered this, right? Hopefully, that was made clear that that can occur.

Another question. Again, I hope this is becoming clearer now, especially having gone through everything, but this question says, "We are a police department for a city. The application needs to be from the city with the police department as the main benefactor?" And that would be accurate. So, again, the city would apply, but how they want to distribute those funds is entirely up to them. And then, the rest of the question, again, I hope this was clear, but "Would the authorized representative be the chief of police or the city manager?" It would be, most likely, your city manager. I don't know for sure, but, again, whoever is the authorized representative for that unit of local government for the city, that's who would need to do the certifications and assurances on the application.

"Is there a list of victim service providers we can contact as possible partners for our application?" That's a really interesting question. There isn't a list. We would hope that because the statute says the local law enforcement grants for the enforcement of cybercrimes you would partner with a local victim service provider. So, this is going to be someone in your community, hopefully, that you're familiar with, maybe even worked with. If you don't know of anyone, a good place to start, and, again, we can maybe talk offline more about this, would be your state domestic violence or sexual assault coalition. But, again, it would be someone in your community. It depends on the breadth of your project too. So, if you're doing something that's state-wide, you might want a state coalition. But if you're doing something that's city or county-wide, you might want a more localized victim service provider as your partner. I'm just saying those are the things to think about, but certainly, if you want to email, we can talk more about that, but there isn't a list.

"Is investigative software considered equipment?" I don't know because I don't know what is considered investigative software. I think when we look at what the statute said, it talks about equipment that's purchased to do the forensic analysis. So, if investigative software is going to help do those forensic analyses, to gather the evidence and do the analysis, whether it's a Cellebrite or whatever it is, then yes, then that's exactly what that is referring to.

This is an interesting question. I'm so glad this came in. "We have a victim services unit within our police department. Are we allowed to still apply?" So, there are two things with that. The first is, remember, police departments are not eligible entities to apply because it's an agency of a unit of local government, which does not qualify. But the other question is really interesting. If you have that victim services unit within a police department, within a prosecutor's office, does that count as the MOU partner is what I'm thinking the question is. And the answer is probably not because of the way a victim service provider is defined. So, the way it's defined in the solicitation and under VAWA,

it really is referring to more of a community-based victim service provider who does direct services as their primary role. So, I would just encourage you to read the definition very closely that's provided in the solicitation and make your decision on who to include as that partner in your application if you choose to apply.

This is a longer one so I might have to take a moment just to scan it. So, there is a question from the Oklahoma State Bureau of Investigation that I may need to come back to that, or we may need to just take this offline in emails because I think it could get a little tricky. What I can say is that the things we're covering today will be more about the application process and not so much the programmatic side of things. So, should you get funded, what can, and can't you do? And I'm not sure that that's where this question from the Oklahoma State Bureau of Investigation was coming from, but just in case, maybe write that into the OVW.cybercrimes email.

Another question out of Dallas. "To clarify, the goal of the MOU is for the police department to partner with a non-profit organization to provide victim services training?" I don't know that that's the only goal and as I mentioned in the presentation OVW really believes in these types of partnerships to provide holistic wraparound services. And so, having that victim service provider as a project partner, not just for the training but really as a partner in all aspects of this project, I think, is going to be beneficial. However, that said, if you read through what Purpose Area 1 talks about and some of the subsections under it, that training for law enforcement -- in fact, let me just get it for you. So, under Purpose Area 1, the training for law enforcement personnel subsection A does say that "provided that the training is developed in collaboration with victim service providers." And so, yes, that's a pretty big point, but as I said earlier, we really want this partnership to be about the whole project.

So, another question. Just a follow-up question, I think, something that had come up earlier. "Does the statute prohibit law enforcement from being the lead applicant?" And yes. Again, any type of agency or unit of government is not eligible to apply. The question goes on to ask, "What is the reasoning?" I don't think I know the reasoning. I just know what the statute says. And so, based on what the statute says, that's how we're implementing the program. But it says, "Since law enforcement can develop and implement the project, oh, it seems strange that we'd be asking another agency to apply." Hopefully, there would be collaboration. I think that's part of the certifications and assurances that everyone involved had an opportunity to review the application and to weigh in on it. But that is what the statute says, so that is how we're rolling out the solicitation.

A question, again, about potentially having a project that focuses only on child victims of cybercrimes. Again, if you read the definition of what a cybercrime is, it talks about the non-consensual distribution of an intimate image of an adult as one of the activities. And so, no, I don't think we can solely focus on child victims. And, again, if we went toward the CSAM area, that's an unallowable activity.

"Will there be requirements for data collection?" Yes. That is in the certifications and assurances. Just like other OVW or DOJ grants, you will be required to do a semi-annual report that you will submit and track various data points. So, that will be a requirement.

And I don't understand, and I apologize, this question about the 50% rule, but again, that's a budget issue, and so, if you were to receive funding, we would probably go back to if you exceeded the 50% on the purchase of equipment.

And I know we're getting close. So, I've gone through a lot of these but there are a couple left. "Can education of the public on cybercrimes against individuals include the education of high school students on crimes other than the distribution of images such as stalking, harassment, and threats made through the use of a computer?" Yes. I think educating the public includes youth as well. Again, if you read what the statute considers a cybercrime, it includes all of those things that you listed. So, I agree. I think that would be permissible.

And we have just one minute. "Can we have the authorized signatory as the chief of police if he is so delegated by the mayor?" I don't know. I'm going to ask that you write in that question. I actually don't know the answer to that. So, please write that in and we'll try to get to the bottom of that.

So, one last question. I know we're right at 3:00. "If a state applies, can the focus be state-wide?" Absolutely. So, your state police can receive those funds. The project can be state-wide and go to different, units of government. Absolutely. There's no geographic limitation to this.

I almost made it through all of the questions. For those of you who didn't, I'm going to try to capture all of these and post them, or if you want, you can write into that OVW.cybercrimes email, that might be the easiest. But since we are at time, I'm going to stop. Thank you so much for really great questions.