SFY 2022-23 Securing Communities Against Hate Crimes (SCAHC) Request For Proposals – Questions and Answers - Posted December 30, 2022

The following questions were sent via email to DCJS through Wednesday, December 14, 2022. Some language has been edited for grammar, clarity and to consolidate similar questions. Please read all questions and responses thoroughly.

A.   General Questions

Question #1: Does DCJS have a definition of a hate crime?

Answer #1: DCJS uses the definition in NYS Penal Law § 485.05, linked **here.**

Question #2: The RFP indicates: "DCJS is committed to funding programs that improve New York's public safety and the effectiveness of New York's justice system. Proposals will be rated and selected for funding consistent with the best interest of the state. Applicants are encouraged to demonstrate in their response to this solicitation how their proposal supports New York's commitment to public safety." What is considered demonstrated support for public safety and the NY justice system? How is the proposal rated if it is in the best interest of the state?

Answer #2: The evaluation and scoring process described in the RFP is designed to ensure that successful applications demonstrate support for public safety and the NY justice system and that the proposal is in the best interest of the state. It also directs that proposals are only submitted that address the RFP purpose.

Question #3: Is this a different funding opportunity from the FEMA Nonprofit Security Grant Program from DHS?

Answer #3:   Yes, this is a separate, state-funded opportunity and is not related to the federal Nonprofit Security Grant Program.

Question #4: Since the submission deadline was changed to February 28, has the project start date also changed?

Answer #4: No, the expected project start date remains 7/1/2023.

Question #5: The application requires a DUNS number but isn't the UEI replacing the DUNS number? In which case, can we use the UEI instead of Duns?

Answer #5: Although the federal government is replacing the DUNS number with the **Unique Entity Identifier,** UEI -- the DUNS number is still required for these state-funded applications. Organizations can request a DUNS number here: https://www.dnb.com/duns-number/get-a-duns.html.

Question # 6: If funding were granted, would acceptance of the funds impose any restrictions on the use or possible sale of the facility? For example, is there anything that would prevent the sale of our building within a certain number of years?

Answer #6: No, the solicitation only requires that security enhancements be to a facility that the organization physically occupies at the time of application and work.

Question #7: When will the application be ready for review and input in Grants Gateway?

Answer #7: Applications for this funding must be submitted in DCJS' Grants Management System (GMS) and will <u>not</u> be processed in the Grants Gateway.

Question #8: Do threats received via telephone, email, or social media qualify as potential risks of hate crime?

Answer #8: Yes, threats received through any medium may be considered as potential risks of hate crime. Applicants must clearly demonstrate how the organization is at risk of hate crime due to its ideology, beliefs, or mission.

Question #9: Is there a limit to the number of attachments we may provide? For example, may we upload a security assessment conducted by an outside firm?

Answer #9: There are no limits to the number of attachments that can be provided. Applicants are welcome to include security assessments conducted by outside firms, but if they are intended to serve as the Vulnerability Assessment, they must have been conducted within the last three years and must be specific to the facility where the security enhancements will take place.

B.   Applicant Eligibility Requirements/Prequalification

Question #1: Can the Streamlined Prequalification Certificate be used for the 2022-23 Securing Communities Against Hate Crimes (SCAHC) grant? How long does it take to get Prequalified through the Grants Gateway?

Answer #1: No, applicants must be prequalified through the NYS Grants Gateway prior to the RFP submission deadline.   There is no streamlined pre-qualification process for this solicitation. Applicants may continue to prepare RFP applications in the Grants Management System (GMS) while applying for and awaiting prequalification. The amount of time needed to get Prequalified through the Grants Gateway varies depending on the completeness of the documentation submitted by the applicant. Applicants are encouraged to start this process right away.

Question #2: One of the eligibility requirements is that the organization be "at risk of hate crimes or attacks because of their ideology, beliefs, or mission." Our organization is not necessarily at risk due to our ideology, but is a theater that hosts a variety performances, many of which could be considered at risk of hate crime. Similarly, as a large venue, we feel that the theater carries an increased risk in general. Would our organization be eligible to apply?

Answer #2: This funding opportunity is limited to not for profit (NFP) applicants. Any NFP applicant who believes their organization is eligible may apply. Final eligibility determinations will be made during application review based on the organizations status as a nonprofit organization that meets all listed eligibility requirements, review of the applicant's response to RFP questions regarding risk of hate crimes, and submission/completion of all required elements of the application. If your organization is otherwise eligible, you must demonstrate in your application why your organization is at

risk of hate crime due to ideology, beliefs or mission. This could include a description of the types of events your organization presents/hosts and why they pose a risk of hate crime.

Question #3: Is our nonprofit (school/church/organization/etc.) eligible to apply?

Answer #3: There are no restrictions on which not for profit (NFP) organizations can submit applications. Final eligibility determinations will be made during application review based on the organizations status as a nonprofit organization that meets all listed eligibility requirements, review of the applicant's response to RFP questions regarding risk of hate crimes, and submission/completion of all required elements of the application. If your organization is otherwise eligible, you must demonstrate in your application why your organization is at risk of hate crime due to ideology, beliefs or mission.

Question #4: Our school, SUNY Canton, submits grant applications in the name of the Research Foundation of SUNY Canton College of Technology. Are we eligible to apply for this grant program?

Answer #4: No, organizations that are part of the SUNY system are not eligible to apply for this current solicitation.

Question #5: Are community colleges eligible for this opportunity?

Answer #5: No, community colleges are part of the SUNY system and are not eligible for this funding opportunity.

Question #6: Is an organization that is exempt from registering with the Charities Bureau based on its incorporation status required to register this exemption with the Charities Bureau?

Answer #6: Yes, although certain organizations are exempt from registering and filing with the Charities Bureau due to their specific incorporation status, exempt organizations must register as exempt so the organization appears in the registry.

Question #7: Can a for-profit landlord apply for funding if space in a building owned by the landlord is being rented to a non-profit?

Answer #7: No, only the non-profit organization would be eligible to apply.

Question #8: My organization applied for the same type of grant last year and was denied. Can I find out why I was denied? How do we apply for this years funding? Does having a previous application denied prevent us from applying for this round?

Answer #8: If you applied to DCJS for the 2021-22 SCAHC funding, the time period for unsuccessful applicants to request a debriefing has lapsed. If you provide a request to dcjsfunding@dcjs.ny.gov with with the details of your application (applicant name, project ID, etc.) DCJS staff can review to determine if any information is available about your application.

To apply for this round of funding, please read through the RFP as well as these questions and answers for information on how to apply. Organizations that were previously unsuccessful applicants are not prevented from submitting an application for the current funding opportunity. Please review all eligibility and submission requirements for this solicitation prior to submitting an application.

Question #9: We have two separate non-profit organizations, with separate EIN and separate certificates of incorporation, however we are sister organizations who share many of the same board members and executive directors. Are we eligible to apply for three grants per organization (to total 6)?

Answer #9: These would be considered two separate organizations and each would be eligible to apply for up to three physical security enhancement projects, plus one cybersecurity project. However, the organizations cannot each apply for the same project at the same facility/building.

Question #10: If a nonprofit landlord rents space to another non-profit, can both organizations receive funding for the same facility? (The landlord uses the building on weekends and the renter during the week).

Answer #10: The two separate organizations can both submit applications for the facility. Both organizations would have to demonstrate their individual risk of hate crime and provide vulnerability assessments and answer RFP questions based on their organization's characteristics. In addition, the projects would have to be separate and distinct- they cannot both submit for the same equipment/type or work at the same facility.

Question #11: If part of the facilities on an organization's campus are under renovation and will not be occupied at the time of application, but will be occupied by the contract start date, is the organization still eligible to apply for campus perimeter protection (fencing, bollards, barriers, etc.)?

Answer #11: If the organization is occupying a portion of the campus at the time of application, the organization is eligible to apply for campus perimeter protection. If the organization is not occupying any of the facilities on the campus at the time of application, it would not be eligible to apply.

Question #12: We are a rural synagogue. As a religious organization, do we have to have documented 501(c)(3) status to apply?

Answer #12: Applicants must either have received a Recognition of Exempt Status Determination Letter from the IRS pursuant to 26 USC §501(c)(3) or must self-certify by providing a letter affirming that the organization qualifies as a 501(c)(3) and is exempt from tax pursuant to 26 USC §501(a).

Question #13: Would two or more nonprofits that have space in the same building be able to submit separate applications for $50,000 each? The entire building has one address but there is an annexed portion.

Answer #13: Yes, separate organizations occupying separate spaces in a building can both apply for separate projects for the portion of the building they occupy. Separate applications cannot be combined to complete a single project type in shared areas in excess of $50,000.

Question #14: Our Diocese oversees several schools. Are we eligible to apply as a district rather than as individual schools?

Answer #14: If the organization is eligible to apply as described in the Applicant Eligibility Requirements section of the RFP, the organization would be eligible to submit up to 3 applications for physical security projects and one application for a cybersecurity project. All applications must be for facilities that the applicant occupies at the time of application, so eligibility to apply on behalf of the schools would depend on the relationship between the schools and the larger organization. DCJS may request additional information to determine that the applicant is eligible to apply for the schools.

Division of Criminal Justice Services

C.   Funding and Award Guidelines/Project Eligibility

Question #1: Is an organization allowed to submit up to three applications for $50,000 for physical security enhancements, plus one additional application for up to $50,000 for cybersecurity (for a possible total of $200,000 in applications)? Or can an applicant only submit up to three applications including a cybersecurity application (for a possible total of $150,000 in applications)? Can an applicant submit only a cybersecurity application, or is a physical security application also required.

Answer #1: Applicants can submit up to three applications for physical security enhancements and/or one application for cybersecurity (for a possible total of four applications for up to $200,000). Applicants do not have to submit a physical security application in order to submit a cybersecurity application, they can submit only a cybersecurity application if they choose. However, only one cybersecurity application is allowed per organization.

Question #2: May we submit three separate physical security projects for a single address or facility?

Answer #2: Yes, for this solicitation applicants can submit up to three applications for physical security enhancements. Applications can be for the same facility/address as long as they are for separate and distinct projects.

Question #3: Our organization is planning to construct a new building or to rehab an existing vacant building we do not yet occupy, with construction to begin at a later date. Is our organization eligible to apply to add security to the new building project?

Answer #3: No, funding is only available for existing facilities that the applicant occupies at the time of application.

Question #4: The RFP states that an organization can apply for up to three physical security projects. How is a project defined? Is a project defined by a complete application with a maximum request of $50,000 which may include different types of equipment for a single facility, or is a project defined by a single type of equipment?

Answer #4: A project can be defined in multiple ways. A project may be a comprehensive security project, which includes several different types of equipment (fencing, security cameras, door hardening, etc.) at a single facility/location. In that case, an applicant may submit up to three distinct applications for up to $50,000 each for comprehensive projects at different locations/facilities.

A project can also be defined as a single category/type of security enhancement, such as fencing or a security camera system at a particular facility/location. In that case, an applicant could submit up to three separate applications for up to $50,000 each for distinct categories of security enhancements.

Each application must be for a single facility/location, but applicants can apply for up to three distinct projects at the same facility/location.   A Vulnerability Assessment must be attached to each application.

Question #5: The RFP states that "Organizations may submit applications for projects at facilities that have received prior DHSES or DCJS SCAHC funding as long as the proposed project is different than any previously funded projects. DCJS may request additional documentation of prior projects to ensure proposed projects are not duplicative". If our organization previously received funding to install a public

address system at one facility, would we now be eligible to install a public address system at a different facility?

Answer #5: Yes, your organization would be eligible to apply for a public address system at a different facility.

Question #6: We have two buildings on our property, but they share the same address. Can we still apply for both buildings?

Answer #6: Yes, an organization with two buildings on the property can submit separate applications for each building as each building would be considered a separate facility and would be eligible for separate projects.

Question #7: Our organization received a previous DHSES or DCJS SCAHC grant for a particular type of equipment (ex. window or door hardening, video surveillance cameras/system). We were unable to complete the project for the entire facility under the budget of that project. Are we eligible to apply to complete that project for the remainder of the facility?

Answer #7: The proposed project may be eligible for funding. The applicant must provide sufficient detail in the responses to the RFP questions, particularly Question #14, to demonstrate that the proposed project is separate and distinct from any previously funded projects.

Question #8: Can a request for equipment that exceeds $50,000 be spread into two applications, or will the grant not fund an improvement that exceed $50,000?

Answer #8: If the equipment requested is a single type (ex. Fencing) at a single facility/location, then the maximum allowed is $50,000. If the total fencing project exceeds $50,000, the applicant can still apply for up to $50,000 and use non-grant funds for the remainder.

If the equipment requested is for distinct types of projects (ex. $40,000 fencing and $20,000 video surveillance system), the applicant can submit separate applications for each equipment type, even if they are at the same facility.

If the equipment requested is a single type (ex. Fencing) but is for separate buildings/facilities, the applicant can also submit separate applications for each facility.

Question #9: Does the cybersecurity application need to be submitted separately from an application for physical hardening equipment, or can we split one application to use some funding for physical hardening and some funding in the same project/application for cybersecurity?

Answer #9: Cybersecurity projects should be submitted as a separate application.

Question #10: Since projects are each for a maximum of $50,000, if we submit one that costs more than $50,000 will it be automatically rejected, will you ask us to reduce the cost to $50,000 or, if you were going to approve it, will you approve it for $50,000 but leave it up to us to fund the balance?

Answer #10: Applications should not exceed $50,000. Applications should reflect the amount of grant funding being requested, up to a maximum of $50,000. If the total cost of a planned project exceeds $50,000, any additional costs would have to be funded by the applicant and should not be included in the application. Applications that request more than $50,000 will still be considered (for funding up to

![New York State Division of Criminal Justice Services logo]

$50,000) but may lose points in the scoring of the budget section, which could impact funding decisions.

Question # 11: Is there any requirement that our facility be handicap accessible in order to receive funding from this program?

Answer #11: There is no specific requirement for handicap accessibility in this funding solicitation, however any renovation/installation/construction must comply with all relevant laws and regulations, which may include requirements for handicap accessibility based on the nature of the project.

Question #12: May equipment be requested for recreational areas that consist of long-term temporary structures including outdoor tents?

Answer #12: Physical security enhancements must be for a facility, which is defined as a building and any adjacent recreation areas. If the recreational area includes a permanent structure, both the structure and the recreational area would be eligible for funding for security enhancements (for example, fencing around the property). However, if the recreational area is on a property with no permanent structures (for example athletic fields with no buildings) that area is not eligible for funding. Tents would not qualify as a permanent structure.

Question #13: Our organization has 10 office locations and when instituting a security measure we set up the same measure across all 10 offices. Is it correct that one application suffices for all 10 offices?

Answer #13: For physical security applications, each separate facility would require a separate application. An organization can apply for up to three projects for physical security enhancements, so you would not be able to complete projects at all ten locations.

For a cybersecurity project, enhancements are likely to be organization-based and can cover multiple facilities in a single application. For example, cybersecurity software or updated servers might be installed in multiple facilities to improve the organization's cybersecurity.

Question #14: Can we submit one application for a single address or property even if it includes more than one building on the property?

Answer #14: Yes, a single address/property can be considered a single facility under one application, even if it contains multiple buildings. You can also choose to identify separate buildings at the same address/property as separate facilities with separate applications if necessary.

Question #15: If an agency has an independent program in a separate building at the same physical address, can they be considered for separate projects?

Answer #15: Organizations can apply for multiple projects at the same facility as long as the projects are separate and distinct.

Question #16: Would an organization be able to apply for installing panic buttons at five different locations (for the same program) as one project?

Answer #16: This depends on how you are defining different locations. If they are different buildings on a single property/campus, they can be included in a single project. If they are completely different locations at separate addresses and not on a single campus, each location would be a separate facility, would require a separate application, and the organization would be limited to three such applications.

Question #17: If we have multiple projects totaling $50,000 is it better to submit separate projects or one application with all of the projects?

Answer #17: This depends on whether the projects are at one facility/location. If, at a single facility, your organization plans to do three projects (for example fencing, lighting, and surveillance cameras) and the total amount is $50,000 or less, you can submit a single application encompassing all three projects. If your organization has three projects at different facilities, you should submit separate applications for each project.

Question #18: For physical security projects, if an organization has a campus facility, does the organization have to submit separate applications for each building or is a separate application only required if buildings are at a different address?

Answer #18: If multiple buildings are on a single campus, the organization can choose whether to submit separate applications for each building (up to 3) or submit a single application for multiple buildings on the campus. If submitting a single application for multiple buildings, the project would be limited to the $50,000 maximum project amount.

Question #19: Can a bungalow colony apply for one application for their synagogue and a second application for the homes where the congregants live?

Answer #19: Organizations can apply for physical security projects at up to three separate facilities, or up to three separate projects at a single facility. In this case, if the organization owns or leases both the synagogue and the residence building(s), the organization can apply for both.

Question #20: If our organization has two neighboring buildings, can we apply for one project to surround both buildings with fencing and another project to replace doors in both buildings?

Answer #20: If the buildings are on the same property, the organization can apply for a fencing project and a door hardening project that would apply to both buildings.

D.   Vulnerability Assessment/Cybersecurity Self-Assessment

Question #1: If we have a vulnerability assessment from a third party which is less than three years old and is still relevant, do we still have to complete the Vulnerability Self-Assessment Tool? Can an organization request a vulnerability assessment from law enforcement, and if so would this carry more weight in the application than the self-assessment?

Answer #1: You may use a third party vulnerability assessment (including one done by a law enforcement agency) which is less than three years old provided that assessment reflects current vulnerabilities and is specific to the facility where the proposed project will be completed. Scoring of the vulnerability assessment is based on how well the assessment identifies potential threats and vulnerabilities of the facility and how well the proposed project relates to those threats and vulnerabilities. The source of the assessment does not impact scoring.

Question #2: The RFP says that to apply for a cybersecurity project, a separate self-vulnerability assessment must be included. Is this the same as the physical security assessment, or is a separate

assessment of cyber vulnerabilities required? Is there a template for the cybersecurity assessment? Are there credential requirements for the organization completing the cybersecurity assessment?

Answer #2: When applying for a cybersecurity project, applicants must include both a Vulnerability Self-Assessment tool for the physical facility/facilities where enhancements will occur, and a separate self-assessment describing the applicant's cybersecurity capabilities and vulnerabilities. There is no template for the cybersecurity self-assessment, organizations should attach a narrative description of the existing cyber capabilities and any vulnerabilities that need to be addressed. There are no credential requirements for agencies conducting the cybersecurity self-assessment, applicants can self-assess or seek an outside assessment at their own discretion.

Question #3: What are definitions of or details about terms in the Vulnerability assessment? For example, what would be the difference between harassment and intimidation?

Answer #3: Applicant's should use commonly accepted definitions of the terms listed in the Vulnerability Assessment. In instances where an applicant is unclear about which term would apply to a particular incident or threat, the applicant has discretion to choose the term that best fits the incident and use the comments area to provide details of the incident.   In the specific case of harassment vs. intimidation, harassment has specific definitions in NYS Penal Law § 240. While intimidation and harassment may include similar characteristics, intimidation would include instances that do not meet the legal criteria for harassment.

Question #4: Is the Vulnerability Assessment used only to determine applicant eligibility or is the Vulnerability Assessment the application itself?

Answer #4: The Vulnerability Assessment is one required component of the application and is used both as part of the determination of applicant eligibility and as part of the scoring of the application itself. Please refer to the RFP for all required components of the application.

Question #5: Is the "separate self-assessment describing the organization's cybersecurity capabilities and vulnerabilities" (page 6 of the RFP) the same as the required "additional narrative description of the organization's current cybersecurity capabilities and vulnerabilities" (page 4 of the RFP)?

Answer #5: Yes, these refer to the same requirement. The Vulnerabiity Self-Assessment Tool must be submitted with each application and the narrative description of the organization's current cybersecurity capabilities and vulnerabilities is required if submitting an application for cybersecurity.

E.   Permissible Costs/Non-Permissible Costs

Question #1: Does a cybersecurity application require that evaluation exercises be a component of the application?

Answer #1: No. Applicants can apply for funding to improve cybersecurity in any of the listed areas, but none are required. All requested items should address vulnerabilities identified in the applicant's self-assessment of it's cybersecurity capabilities and vulnerabilities.

Question #2: Our organization has recently initiated first steps toward improving our cybersecurity. Will DCJS consider both ongoing and new efforts in this direction?

Answer #2: All eligible expenses must have been incurred post-award and during the term of the grant contract. The expected contract start date is 7/1/23, so any purchases made or expenses occurred prior to that date would be ineligible. Grant funding must be used to supplement, not supplant, non-grant funds that would otherwise be available for expenditure on the proposed project. As such, any item/enhancement that your organization has already committed to funding from another source would be ineligible for grant funding. Enhancements or components of a cybersecurity project that are additional to what was previously planned are eligible.

Question #3: Our facility has a set of entry doors leading directly into the building. We would like to create a mantrap door system but we do not have sufficient space in the building. Is it allowable to build a second set of doors outside the current entrance to allow for a mantrap system, even if no framing currently exists for additional doors?

Answer #3: Yes, this would be considered an alteration to an existing structure to allow for door hardening and is allowable.

Question #4: The RFP states that grant funds cannot be used to fund personnel. However, could grant funding be used to hire contracted security guards (not employees, but contractors)? Would they have to be new guards, or could the funds support contracted security guards that we contracted with in 2022 already?

Answer #4: No, the funds cannot be used to hire/contract security guards. Funds in physical security applications are for physical security enhancements to the facility or training only.

Question #5: a. Our organization is currently using computers that are 6-7 years old and not compatible with Windows 11. This means that we will be using computers that will be out of date with security patches and vulnerable to cyber-attacks. Can we use grant funding to purchase docking stations and laptops that are capable of running security patches and software that protects against cyber-attacks?

b. In the event of a power failure at our main facility, our cybersecurity defense mechanisms go down. Would we be able to use grant funds to install a power generator for our main facility?

Answer #5: The items listed are not explicitly prohibited and therefore would be considered for funding. As is the case in all cybersecurity applications, the applicant would be expected to sufficiently describe the organization's current capabilities and vulnerabilities and demonstrate how the proposed purchase would address those vulnerabilities.

Question #6: Is this funding allowed to be used to create a guard booth at the driveway entrance? This is a necessary security need because the entrance is so far away from a building on the property that it makes it difficult to have a security guard on site during inclement weather or to manage traffic entering the site.

Answer #6: No, a guard booth would be considered an ancillary construction cost which is listed as an ineligible expense.

Question #7: Would the purchase of a vehicle intended for security patrolling of an organization's property be an allowable expense?

Answer #7: No, allowable expenses are physical security enhancements to the facility. A vehicle is not an allowable purchase.

Question #8: Is security planning an eligible item to request for target hardening?

Answer #8: No, expenses for the development of a security plan, risk assessment, or vulnerability assessment are not eligible. Expenses related to training of staff or participants in security procedures or practices are eligible.

Question #9: In November 2022, the Governor announced this grant as part of legislation that was signed to "promote educational initiatives, which serve as key tools to further tolerance and acceptance, and in turn help keep communities safe from hateful acts and violence." Is tolerance education an eligible expense?

Answer #9: Funding is limited to physical facility hardening, security training, and cybersecurity as described in the RFP. Tolerance education would only be allowed as part of a training program for staff and organization members that is designed to improve security of the organization.

Question #10: For cybersecurity applications, can a proposal be sent in requesting $50,000 for a professional assessment from a cybersecurity firm with the balance to be used to carry out any recommendations made to enhance our networks security?

Answer #10: For cybersecurity projects, planning and assessment costs are allowable expenses. Applicants are encouraged to research the approximate cost of such planning/assessment so the proposal reflects expected costs as accurately as possible and budgeted items are reasonable. When the approximate expected cost of planning/assessment has been determined, the remaining funds could be designated for implementation of recommended enhancements.

Question #11: Are costs for interior emergency lighting eligible expenses? Is a generator or other items listed on the Federal NSGP AEL list eligible? Are costs for alarm monitoring, storage and retrieval of alarm data/video allowed?

Answer #11: Any item not specifically listed under ineligible expenses is potentially allowable. Final determinations of expense eligibility will depend on the justification of the expense and its relation to the threats and vulnerabilities identified in the vulnerability assessment and in the RFP questions.

Question #12: Does the implementation of an Artificial Intelligence solution to prevent hate-based cyber disruption (SPAM, Phishing filtering) qualify for cybersecurity funding?

Question #12: Any item not specifically listed under ineligible expenses is potentially allowable. Final determinations of expense eligibility will depend on the justification of the expense and its relation to the threats and vulnerabilities identified in the vulnerability assessment and in the RFP questions.

Question #13: With regard to physical security training costs, will funds support the implementation of a train-the-trainer program in which one of our lead security/safety officers trains a small group of employees who then train all staff within a facility?

Answer #13: Yes, this is allowable as long as the costs of the training program are otherwise eligible expenses. Personnel costs for staff members providing the training are not eligible expenses.

Question #14: Please define Ancillary Construction costs. If a project requires modifications to a space, for example to install shatter proof windows, is that considered a prohibited ancillary construction cost?

Answer #14: For the purposes of this solicitation, ancillary construction costs refer to the building of additional structures not already in place (such as a guard booth at the property entrance) or construction costs not directly related to/required for the facility hardening project. Modifications to existing structures that are necessary to complete the physical security project would be allowed (for example, modifying the facility entrance to allow for access control or a mantrap entrance, or modification of windows to allow for installation of shatterproof glass).

Question #15: Some cybersecurity costs are one-time expenses, while others are recurring costs (such as dark web monitoring, network intrusion detection, etc.). If these expenses can be costed out to an annual figure for the term of the contract, can they be included?

Answer #15: Yes, recurring costs for cybersecurity monitoring or software licenses can be included, but must be for expenses incurred during the contract period.

Question #16: Are the following items considered eligible items to strengthen safety and security?

a. Lighting infrastructure

b. Entrance gate

c. Garage/shed to store assets

Answer #16: The first two items listed (lighting infrastructure and entrance gate) are generally eligible expenses. The final determination of eligibility would depend on the justification of the expense and how its relation to the threats and vulnerabilities identified in the vulnerability assessment and in the responses to the RFP questions. The final item (garage/shed) would be a new structure and would be considered a prohibited ancillary construction cost, and not eligible

Question #17: Is cybersecurity for organization-owned cell phones eligible? Is an Endpoint detection and response (EDR) eligible? Is funding available for cybersecurity subscription services such as phishing testing, education, cloud backup services, IT support, or software licensing?

Answer #17: Any item not specifically listed under ineligible expenses is potentially allowable. Final determinations of expense eligibility will depend on the justification of the expense and its relation to the threats and vulnerabilities identified in the vulnerability assessment and in the RFP questions.

Question #18: Can you provide more information about which cybersecurity trainings are eligible? Can we use a cybersecurity assessment from our own IT department? Can we use our own IT staff for cybersecurity?

Answer #18: For cybersecurity applications, it is up to the applicant to identify cybersecurity trainings based on the organization's identified cybersecurity vulnerability and needs. Proposed trainings should be sufficiently justified in the budget and responses to RFP questions and should relate to the vulnerabilities identified in the self-assessment of cybersecurity capabilities and vulnerabilities.

Applicants can use a cybersecurity assessment from their own IT department as long as it describes the organization's current cybersecurity capabilities and vulnerabilities. Applicant's can use their own IT staff to conduct training or to implement cybersecurity enhancements, but grant funds cannot be used to pay personnel expenses for the work of in-house staff.

F.   Evaluation of Applications/Scoring

Question #1: Would multiple applications for the same facility be scored by the same reviewers?

Answer #1: Reviewer assignments will be determined based on a number of factors after all applications have been received, but it is expected that all applications from a particular organization will be scored by the same reviewers in order to ensure that the projects are separate and distinct projects.

G.   Request for Proposal Questions/Narrative Responses/Budget and Work Plan

Question #1: The RFP says cybersecurity applications will require an additional narrative (page 4). If the whole application project is for cybersecurity, then would the standard application with 14 questions be submitted and the focus for questions 8 and 11 that request information on the project investment will just describe the cybersecurity investment? Or is there another separate narrative that needs to be attached?

Answer #1: Each application requires only one set of responses to the RFP questions. The separate narrative required for cybersecurity applications refers to a **self-assessment of the organizations cybersecurity capabilities and vulnerabilities**. For cybersecurity applications, this self-assessment should be in addition to the Vulnerability Self-assessment form for the facility/facilities where cybersecurity enhancements will be housed/installed.

Question #2: If our organization previously received a FEMA NSGP award, should the information on the award and equipment installed be included in the response in question 14?

Answer #2: No, applicants are only required to provide information on awards received through the Securing Communities Against Hate Crimes program, administered either by NYS DHSES or NYS DCJS.

Question #3: One of the questions asks for the number of events at the facility. Does this include the number of cyber events? Should the number of cyber events be included for cybersecurity applications? Please define events? Are meetings considered events?

Answer #3: No, the question is referring to events with in-person attendance at the facility. Virtual attendance should not be included. Events include any instance where the organization is hosting multiple members of the public or of other organizations for a purpose outside of the day-to-day operations of the facility. For cybersecurity applications, applicants should respond with the number of in-person events held at any/all facilities where cybersecurity enhancements will occur.

Question #4: Should applicants create a word document to copy and paste into GMS by copying the RFP questions on pages 11-15 of the RFP?

Answer #4: Applicants should create a word document that includes the answers to the questions in the RFP. Applicants can then copy and paste each response from that word document into the appropriate question in the Questions tab in GMS. Finally, applicants should attach the word document in GMS using the Attachments link. This creates a backup of the responses in cases there are any difficulties with the answers submitted directly in GMS.

Question #5: For the question on maximum number of occupants on site, should we include pre-covid numbers?

Answer #5: Yes, the answer should include the maximum number of occupants during normal operations of the facility.

Question #6: For question #5 regarding the Vulnerability Self Assessment Tool, should we just answer see attached? On the Vulnerability Assessment Tool, how should we link the threats to the vulnerabilities as the comments section is limited?

Answer #6: If there is insufficient space to provide the information on the Vulnerability Assessment Tool, applicants can provide additional information in the answer to question #5 in GMS and on the corresponding word document with RFP question responses. Please indicate "see attached Word Document for additional information" in the GMS.

Question # 7: When entering items in the budget, should we list an equipment type/category as 1 system, or should we provide unit numbers? For example, should the budget line say 1 camera system, or should it indicate 15 cameras at a particular price per unit?

Answer #7: The budget line should be for a particular equipment type (such as video surveillance system), while the justification for that line should include specific detail about the number of cameras or other items to be included.

Question #8: Are guidelines available to characterize reasonable and appropriate budget costs?

Answer #8: There are no specific guidelines available as each project will be unique and the cost of common items can fluctuate. Applicants are encouraged to seek multiple informal quotes/estimates for proposed items/projects to ensure the proposed budget reflects reasonable costs at the time of application.

Question #9: What does the following mean: "For subcontracted agencies approved to provide services, where applicable, upload signed and executed agreements and the subcontractor's approved operating budget using the Attachment Tab on GMS."

Answer #9: This refers to grant programs where grant recipients may subcontract a portion of the funds to another agency/organization to provide a portion of the services funded by the grant. It is unlikely that this statement will apply to this grant program as grantees are receiving grant funded equipment or services rather than using grant funds to provide a service.

Question #10: What are line, word, and character limits for RFP question responses and Vulnerability Assessment comments?

Answer #10: Although the Vulnerability Assessment and/or GMS may have word or character limits, there are none specificied in the RFP. If an applicant is unable to fit a response or comment within the character limits imposed by the system or document, the applicant can indicate see attached and attach a separate word document in GMS with the full response.

Question #11: Our organization is planning to submit a physical security application for CCTV and a cybersecurity application for equipment and training. Which budget categories should we use for these items?

Answer #11: Any physical security equipment that requires physical installation at the facility, such as CCTV cameras/system, should be entered in the Alterations and Renovations category. Equipment that does not require installation, such as hand held radios and most cybersecurity equipment (servers, software, etc.), should be entered in the Equipment category. Training expenses should be entered either under Consultants (if the organization is hiring an outside consultant to provide training), Supplies (if the organization is purchasing a training program or materials to deliver training), or All Other Expenses (if the organization is paying registration expenses for staff/members to attend training).

Question #12: For the work plan, if an organization is planning to purchase equipment only, is Objective 2 regarding training still required? Performance number 3 is very unclear.

Answer #12: All applicants should enter the Standardized work plan for their project (either physical security or cybersecurity) as written. If an applicant receives an award, program representatives will be available to assist in explaining work plan objectives, tasks, and performance measures as necessary.

Question #13: For the work plan, how should we build in potential delays to equipment purchase due to supply chain issues?

Answer #13: Applicants should be using the Standardized Work Plan provided in the RFP. After award notification and contract execution, the work plan will be used to develop quarterly progress reports where the grantee will be able to document and describe any delays in project implementation.

H.   Notification of Awards/Administration of Contracts/Submission Requirements

Question #1: Is this program awarded on a rolling basis, so it is awarded on a first-come first-served basis until all funds are awarded or the funding deadline is reached?

Answer #1: The method of determining and announcing awards will be finalized after an analysis of the applications received by the application deadline. However, the goal is to issue award notifications as soon as possible after the deadline.

Question #2: On p. 19 of the RFP, you state: "Bidders/applicants can demonstrate their commitment to the use of Service Disabled Veteran Owned Business (SDVOB) by responding to the questions on the form located here and attach the completed form……" When we click on "here", we get a message – Page Not Found.

Answer #2: Here is an updated link to the Service Disabled Veteran-Owned Business Utilization plan form: https://ogs.ny.gov/veterans/division-service-disabled-veterans-business-development-compliance-and-reporting

The form is available under Contractor Reporting Forms, form SDVOB100.

Question #3: If we are submitting more than one application, must we complete the Vendor Responsibility Questionnaire prior to application submission?

Answer #3: Organizations are only required to submit a Vendor Responsibility Questionnaire for applications greater than $100,000. Since this solicitation only allows individual applications of up to $50,000, applicants are not required to submit a Vendor Responsibility Questionnaire. However, DCJS is required to complete a Vendor Responsibility evaluation for all contracts, so completion of a Questionnaire is encouraged although not required.

Question #4: Can you confirm whether the following forms are required with submission?

   a. Sexual Harassment Prevention Certification
   b. Encouraging Use of New York State Businesses in Contract Performance
   c. Veteran Owned Business Form
   d. MWBE- DCJS 3301 and MWBE 3309

Answer #4:

   a. The Sexual Harassment Prevention Certificate is required with application submission.
   b. The Encouraging Use of New York State Businesses in Contract Performance form is required with application submission.
   c. The Service-Disabled Veteran Owned Business (SDVOB) form is not required but participation with SDVOBS is strongly encouraged and can be demonstrated using the form. An updated link is provided here: https://ogs.ny.gov/veterans/division-service-disabled-veterans-business-development-compliance-and-reporting
   d. MWBE DCJS 3301 and DCJS 3309 forms are not required with the application, but will be required post-award for any grant contracts that exceed $25,000.   Applicants are encouraged to research the availability of MWBE providers for proposed projects in order to facilitate contract development and can provide the forms with their application.

Question # 5: A required attachment is the Encouraging Use of New York State Businesses in Contract Performance. I have some questions on this document:

   a. If we want to use NYS businesses but we don't have any specific business in mind should we still mark the form as yes and just leave the list of businesses empty?

   b. If we have specific businesses we know about and we list it on this document, are we unable to solicit bids to other businesses? Are we restricted to using these businesses?

   c. Is it against procurement rules to list businesses (so if we write any businesses down then we are not allowed to work with them)?

NEW YORK STATE | Division of Criminal Justice Services

Answer #5:
    a. Yes, you can still mark yes that you intend to use NYS businesses and indicate To Be Determined in the list of businesses.
    b. No, this is not a formal commitment to use those businesses, merely an indication of intent. This does not prevent organizations from soliciting other bids or using other vendors.
    c. No, indicating your intent to use particular businesses on this form does not violate procurement rules. Applicants will still have to comply with procurement requirements indicated in the grant contract regardless of which vendors are listed on this form.

Question #6: Aside from the vulnerability assessment and the photo of the facility along with documentation in regards to any threats, is there any other documentation such as price per cost required for the submission?

Answer #6: The submission requirements are delineated in the Application Checklist on page 22 of the RFP. Please read the RFP thoroughly for details related to each requirement.

Question #7: The standard contract language indicates that purchases in excess of $10,000 require a competitive bidding process. Are three bids required to purchase equipment? Does the organization have to show proof of the bidding process in the application, or is it only required after an award is issued?

Answer #7: Procurement requirements are described in the standard contract language linked in the RFP and are dependent on the aggregate dollar amount of the purchase. Applicants are not required to document the bidding process or other procurement processes at the time of application. Applicants should consider the procurement requirements when planning projects and must follow all contract terms and conditions if awarded funds.

Question #8: Regarding the MWBE requirements, if an organization submits three applications, each for less than $25,000 does the MWBE requirement still apply based on the total of the applications?

Answer #8: No, the MWBE requirements are specific to each application and subsequent grant contract. Applications/awards for $25,000 or less are not subject to MWBE requirements.

Question #9: The MWBE requirements say that 30% of the award must be spent with MWBE providers, but if a project is for a single type of equipment it may not be possible/feasible to split the spending among different vendors. In this case it would appear that the entire award amount would have to be spent with MWBE providers. In past instances, MWBE providers have been unresponsive or lack the required commodity codes for the items needed. How is this handled?

Answer #9: MWBE requirements apply to the portion of the project budget that is determined to be discretionary. During contract development, grantees will evaluate each budget item/purchase to determine if an MWBE provider is available and capable of providing the each item. If all potential MWBE providers are unresponsive or unable to provide particular items, those items would be excluded from the discretionary budget and would not be subject to the 30% MWBE spending requirement.

I.   Grants Management System(GMS)

Question #1: Can the Primary and Signatory contacts in GMS be the same person?

Answer #1: Yes.

Question #2: Which fields are required in the Participants tab in GMS?

Answer #2: All fields with asterisk are required for GMS to allow submission of an application. Some additional fields may become required by the system based on selections made by the applicant. Applicants should provide information in all fields that are applicable to their organization.

Question #3: The tutorials on the GMS site require Adobe Flash, which is no longer supported. Is there a workaround so we can view these tutorials?

Answer #3: The link to the tutorials on the GMS home page was left on the page in error and will be removed. For guidance on GMS, applicants should refer to the GMS Application manual, available here: https://www.criminaljustice.ny.gov/ofpa/applcntgrntfrms.html .

Question #4:   Is the NYS Vendor ID # the same as the SFS Vendor ID #?

Answer #4: Yes, the NYS Vendor ID# referenced in GMS is the same as the SFS Vendor ID #.