



Request for Applications (RFA)

for

the 2026 Securing Communities Against Hate Crimes (SCAHC) Grant Program

Kathy Hochul, Governor

Rossana Rosado, Commissioner

Key Dates and Notices

RFA Release Date	Wednesday April 15, 2026
Application Due Date:	Wednesday July 8, 2026, at 12:00 p.m. (noon) EST
Estimated Total Program Funding	Up to \$70 million*
Award Ceiling	\$250,000
Anticipated Number of Awards	140-280
Deadline for Final Submission of Questions	Wednesday May 6, 2026
Response to Questions Posted	on or about Friday May 29, 2026
Notification of Award(s)	Wednesday September 2, 2026
Anticipated Contract Start Date	January 1, 2027

* \$35 million from FY 2026 Enacted Budget with the additional amount subject to appropriation in the FY 2027 Enacted Budget.

FY 2026 Securing Communities Against Hate Crimes (SCAHC)

Request for Applications

Table of Contents

I. INTRODUCTION AND GENERAL INFORMATION.....	4
II. PROCUREMENT REQUIREMENTS – GUIDELINES – VENDOR SELECTION.....	5
III. FUNDING, APPLICANT ELIGIBILITY AND CONTRACT TERM	7
A. Funding and Award Guidelines.....	7
B. Applicant Eligibility Requirements.....	8
C. Availability and Approved Use of State Funds	9
D. Contract Term.....	9
IV. PROJECT DESCRIPTION	9
V. BEST PRACTICES AND REFERENCE MATERIALS	13
A. Best Practices.....	13
• Appendix - Best Practice for Preparing an Effective Grant Application	
• Appendix - Best Practice Guide for Securing your Facility	
B. Reference Materials.....	13
• Appendix - State and Federal Resources for Facility Security	
VI. EVALUATION AND SELECTION OF APPLICATIONS.....	13
Tier I Evaluation	13
Tier II Evaluation.....	15
Tier III Evaluation.....	15
VII. REQUEST FOR APPLICATIONS QUESTIONS	16
VIII. NOTIFICATION OF AWARDS	21
IX. REPORTING REQUIREMENTS	22
X. ADMINISTRATION OF CONTRACTS	22
XI. APPLICATION SUBMISSION AND REQUIREMENTS.....	28
XII. APPLICATION CHECKLIST.....	29

APPENDICES:

- [SFS Prequalification Requirement.](#)
- [DCJS Grants Management System \(GMS\) Instructions and Helpful Hints.](#)
- [Best Practices for Preparing an Effective Grant Application.](#)
- [Best Practice Guide for Securing Your Facility.](#)
- [State and Federal Resources for Facility Security.](#)
- [Resources for Nonprofit Cybersecurity Projects.](#)
- [Reported Hate Crime Incidents Per County Data.](#)
- [Standardized Work Plan.](#)
- [Budget Detail Worksheet and Narrative Guide.](#)

ATTACHMENTS REQUIRED IN GMS:

- Attachment 1 -Vulnerability Self-Assessment Tool (PDF download available on our [website](#))

I. INTRODUCTION AND GENERAL INFORMATION

The New York State Division of Criminal Justice Services (DCJS) seeks applications to fund safety and security projects at nonprofit organizations at risk of hate crimes or attacks because of their ideology, beliefs, or mission. Approximately \$35 million to \$70 million is expected to be made available to fund approximately 140-280 projects throughout New York State.

Hate crimes target individuals, groups of individuals, or property because of a belief or perception regarding the race, color, national origin, ancestry, gender, gender identity or expression, religion, religious practice, age, disability or sexual orientation of a person, as defined in Article 485 of the Penal Law. The total number of hate crime incidents reported to police represents a fraction of all reported crime in the state. However, despite hate crimes targeting individuals or individual structures, these crimes can adversely affect entire communities. New York State tracks these incidents separately from other crimes so trends can be monitored, and to allow the state to be proactive in efforts to prevent hate crimes and ensure the safety and equal treatment of all New Yorkers.

Through this Request for Applications (RFA), DCJS seeks to strengthen safety and security arrangements at the facilities of New York nonprofit organizations at risk of hate crimes or attacks, including virtually or on the internet, because of their ideology, beliefs, or mission. Grants awarded upon the culmination of this process will be administered by DCJS.

DCJS enhances public safety by providing resources and services that inform decision making and improve the quality of the criminal justice system. DCJS is a multi-function criminal justice support agency with a variety of responsibilities, including collection and analysis of statewide crime data; operation of the DNA databank and criminal fingerprint files; administration of federal and state criminal justice funds; and the identification and funding of programs that reduce crime, recidivism, and victimization.

DCJS is committed to funding programs that improve New York's public safety and the effectiveness of New York's justice system. Applications 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 application supports New York's commitment to public safety.

Please Note:

1. Applications must be received by the submission deadline on-line via the DCJS Grants Management System (GMS). **Applicants who are not registered to access GMS will need to obtain user access to respond to this Solicitation.**
 - Please see [Appendix: DCJS Grants Management System \(GMS\) Instructions and Helpful Hints](#).
2. Questions regarding this RFA must be emailed to dcjsfunding@dcjs.ny.gov. Responses to the

questions will be posted on the DCJS [website](#) on or about the date indicated above. If the applicant has any general questions such as, “Did DCJS receive my e-mail?” please call (518) 457-9787. **Please note that DCJS cannot answer substantive questions concerning this solicitation in any manner other than the e-mail method.** This is to ensure equity in the application process and that all applicants have access to the same information.

3. Applicants will be advised of award decisions via a letter of notification, which will be emailed to the address provided by applicant in GMS. Where applicable, applicants not receiving an award will receive notification via email to the contact email provided in GMS. A debriefing is available to any entity that applied in response to this solicitation who is not successful in receiving an award. (See Section: Notification of Awards.) Unless otherwise modified by DCJS, the anticipated contract period for this grant opportunity will be for 24 months, with a tentative start date of January 1, 2027.
4. **Prequalification** – To be considered for an award, not-for-profit (NFP) applicants **must** be pre-qualified prior to the RFA submission deadline. Please see [Appendix: SFS Prequalification Requirement](#)

II. PROCUREMENT REQUIREMENTS – GUIDELINES – VENDOR SELECTION

Procurement Guidelines:

Please ensure that the proper procurement guidelines are followed when procuring vendors. It is necessary to ensure that all documentation about how a vendor(s) has been procured and justification for reasonableness of cost is maintained and can be provided to DCJS staff upon request. Please see retention requirements in the [Records](#) section. Failure to comply with procurement guidelines may result in disallowance of costs, voucher rejections, and/or termination of contract(s).

Please note, any and all vendors/subcontractors must have all the necessary licenses, approvals, and certifications currently required by the laws of any applicable local, state, or Federal government to perform the services or work, as applicable.

Not For Profits:

If the Grantee is eligible to purchase an item or service from a government contract (such as a New York State Office of General Services (OGS) contract) or is able to purchase such item or service elsewhere at a lower than or equal price, they do not need to follow the below procurement guidelines, but instead, if purchasing off an OGS contract, grantees must follow the OGS How-to-Use-Guidelines linked below.

Please see the following Helpful Resources information.

Helpful Resources:

Below are links to an OGS contract with an approved list of vendors for Facility and Security System enhancements, as well as How to Use Guidelines.

- [Contractor Information Summary](#)
- [OGS Contract How-to-Use Guidelines](#)

Purchases up to \$5,000

- Grantee may purchase any single piece of equipment, single service or multiples of each, that cost up to \$5,000 at their discretion.
- Please Note: MWBE goals still apply.

Purchases between \$5,000-\$50,000

- Grantee must first obtain at least 3 written quotes on the vendor's stationery prior to the purchase. Please note that emailed quotes or quotes received electronically are sufficient as long as it is clear from which vendor it originated and includes sufficient detail.
- For purchases over \$25,000 DCJS recommends, but does not require, that quotes be solicited via an advertisement or soliciting a large group of appropriate vendors/contractors to demonstrate appropriate market rate.
- Grantee must maintain a record of the quotes obtained.
- Please Note: MWBE goals still apply.

Purchases over \$50,000

- Grantee must utilize a competitive bidding process.
- Please Note: MWBE goals still apply.

Competitive Bidding Procurement Process (must include):

- Open and fair solicitation of the opportunity to provide services.
- Information provided equally to all interested parties.
- Solicitation lists reasonable deadlines for interested applicants.
- A methodology for evaluating bids must be consistently applied to all applicants.
- A justification for which bid was selected must be recorded to justify the selection.

- Maintenance of a record of the competitive procurement process for audit purposes.

Any grantee who proposes to purchase from a vendor without competitive bidding, above the \$50,000 threshold, or who believes they have a justification for not following the processes detailed above for purchases under \$50,000, must obtain the prior written approval of DCJS in the form of an approved [Single/Sole Source Authorization Form](#).

- The circumstances leading to the selection of the vendor/contractor, including the alternatives considered and the rationale for selecting the specific vendor/contractor, must be included in the single/sole request. It must also include the method for determining the reasonableness of cost
- Proof of reasonableness of cost must be documented. An example of this would be to obtain price quotes from other vendors or contracts from the selected vendor within the past two years.
- Ensure selected vendor(s) are qualified (licensed and/or certified where applicable) consistent with New York State contractual requirements.
- Please note that the burden for justification falls on the grantee and approval is not guaranteed.

III. FUNDING, APPLICANT ELIGIBILITY AND CONTRACT TERM

A. Funding and Award Guidelines

DCJS expects that \$35-\$70 million will be made available to support approximately 140-280 projects. Applications will be accepted for up to \$250,000 **per organization**. Each eligible organization may submit one (1) application for one or more physical security enhancements and/or cybersecurity enhancements.

Organizations can submit for different types of enhancements within their application (e.g., locks and alarm system) so long as the total requested by the organization is equal to, or less than, \$250,000. Organizations may submit applications for projects at facilities that have received prior Division of Homeland Security and Emergency Services (DHSES) or DCJS SCAHC funding if the proposed project is different than any previously funded projects or build upon or enhances the security measures previously undertaken.

All applicants will be required to attest, in response to the RFA questions, that the proposed project is separate and distinct from any previously funded projects and that none of the requested items/services have been funded by another grant or funding source. DCJS may request additional documentation of prior projects to ensure proposed projects are not duplicative.

Applications that include cybersecurity projects will require an additional narrative description of the organization's current cybersecurity capabilities and vulnerabilities, which should be attached to the application as a Word document or PDF.

All funding must support project-related costs that will be incurred during the contract period. Funding under this program must supplement, not supplant, non-grant funds that would otherwise be available.

B. Applicant Eligibility Requirements

This RFA requests applications to support projects that enhance the safety and security of nonprofit organizations at risk of hate crimes or attacks due to their ideology, beliefs, or mission. Nonprofit organizations that have received prior DHSES or DCJS SCAHC funding are eligible to apply for additional funding if the proposed project is different than any previously funded projects or build upon or enhances the security measures previously undertaken. Each applicant must be pre-qualified in the New York Statewide Financial System (SFS). Please see [Appendix: SFS Prequalification Requirement](#) for instructions on how to become pre-qualified.

To be eligible, applicants must meet **all** the following requirements:

- Have received a Recognition of Exempt Status Determination letter from the IRS pursuant to 26 USC §501(c)(3). Alternatively, the applicant may self-certify by providing a letter affirming that the organization qualifies as a §501(c)(3) organization and is tax-exempt pursuant to 26 USC §501(a). The organization must maintain tax exempt status throughout the life of the grant. If the organization's tax- exempt status is jeopardized or placed into question at any point during the life of the grant, the organization must notify DCJS within fifteen (15) days.
- Be a nonprofit organization.
- Be at risk of a hate crime or attack due to ideology, beliefs, or mission as described by the applicant organization and consistent with New York State law be registered, have recently applied for registration and such application remains pending, or be exempt from registering with the NYS Attorney General's Office, Charities Bureau.
 - Exempt organizations must provide a signed attestation on organization letterhead affirming that the organization is exempt from registering and explaining the reason for exemption pursuant to Executive Law Article 7A and/or Estates, Powers, and Trusts Law (EPTL).
- Be prequalified through the [New York Statewide Financial System \(SFS\)](#) **at the time of application.**

C. Availability and Approved Use of State Funds

Grant funding will be awarded competitively for allowable interior and exterior facility hardening, physical security enhancements, cyber security enhancements, and training of staff or organization members in the use of the security equipment or cyber security enhancements to harden nonprofit facilities at risk of hate crimes.

Staff or personnel costs are **NOT** allowable given the funding source used to support this grant program (Capital Funding). Applications must be for new projects, or projects that build upon or enhance the security measures previously undertaken. Grant funds cannot be used to support projects that have been undertaken prior to award or outside the period of the grant contract. Grant funds may not be used to fund projects that have already been reimbursed through any other grant program, including but not limited to the Non-public Safety Equipment (NPSE) Program administered by the State Education Department, or the Nonprofit Security Grant Program (NSGP) administered by DHSES, or DCJS.

The Securing Communities Against Hate Crimes Program (SCAHC) advances a common understanding of risk management, i.e., identification of risks and vulnerabilities and associated methods of reducing and/or eliminating those risks and vulnerabilities. Applicants must submit a facility-specific Vulnerability Self-Assessment which describes relevant threats and security vulnerabilities and describes how the organization will prevent and protect against hate crimes or attacks targeting their facility. Applications must request funding for projects/activities which will mitigate those risks and vulnerabilities as identified in the *Vulnerability Self-Assessment Tool*.

Applicants seeking funding for a project to improve cybersecurity must also provide an attachment in GMS describing their assessment of the organization's current cybersecurity capabilities and vulnerabilities.

D. Contract Term

Unless otherwise modified by DCJS, the anticipated contract period for this grant opportunity will be for 24 months, with a tentative start date of January 1, 2027.

IV. PROJECT DESCRIPTION

A. Vulnerability Self-Assessment

1. Applicants must submit a completed application and include a Vulnerability Assessment for **each** facility for which grant funding is requested. The Vulnerability Assessment shall identify threats to the facility as well as physical and/or human security vulnerabilities. Applicants must use the *Vulnerability Self-Assessment Tool* included with this RFA to satisfy the Vulnerability Assessment requirement for a

physical security enhancement and/or training. If your organization has a Vulnerability Assessment that has been completed within the past year, it may be used to satisfy this requirement provided that the assessment reflects current vulnerabilities of the facility.

2. An applicant submitting an application that includes a cybersecurity project will be required to submit a separate self-assessment describing the organization's cybersecurity capabilities and vulnerabilities. The cybersecurity self-assessment should be labeled *Cybersecurity Self-Assessment* and must be attached in GMS as a Word document or PDF.

B. Permissible Costs

The SCAHC application must describe the new elements requested for funding to directly address risks and vulnerabilities as identified in the Vulnerability Assessment.

Permissible costs to protect against potential hate crime activity include:

- hardening the organization's facility, including areas adjacent to the facility, through exterior and/or interior physical security enhancement; and/or
- providing security training that will advance the knowledge of security personnel, staff, and membership as appropriate.
 - *If a paid trainer is to deliver training, the cost should be listed in the budget category "Consultants." Training materials should be listed under the "Supplies" budget category.*

1. Facility Hardening Costs

Permissible costs include both internal and external facility hardening structures, devices or equipment that mitigate vulnerabilities identified in the Vulnerability Assessment. Funding can be used for the acquisition and installation of security equipment on real property/existing facilities owned or leased by the nonprofit organization, specifically for prevention of, and/or protection against, hate crimes. Any applicant who proposes work on a leased property is exclusively responsible for ensuring compliance with the landlord lease agreement and associated requirements, particularly regarding structural alterations, equipment installations, and any alterations made with grant funds. Additionally, the applicant/grantee is solely responsible for compliance with all State and local permitting or environmental compliance requirements, including ensuring appropriate licensure for any vendors or individuals performing work supported through the SCAHC program.

Security enhancements must be for a facility or facilities that the organization

physically occupies at the time of application. Please note that should you apply for enhancements or projects at a specific facility, you will only be permitted to conduct work at the facility identified in the application for that specific project.

Allowable equipment consists of, but is not limited to, the following external and internal facility hardening projects:

- Perimeter lighting.
- Alarm systems.
- Camera-based security systems.
- Access control systems.
- Perimeter fencing, barriers, bollards.
- Blast resistant film for windows and/or shatter resistant windows.
- Interior and exterior doors and hardening/locking mechanisms.
- Panic Button/Lock-Down systems.
- Public Address (PA) Systems.
- Impact protection.

Please refer to [Appendix: Best Practice Guide for Securing Your Facility](#) for further guidance on recommended security considerations and enhancements.

2. Security Training Costs

The SCAHC Program for nonprofit organizations allows costs to train security personnel and other appropriate staff or organization members to prevent and protect against hate crimes. Allowable training topics are limited to the protection of physical security; training that will advance the knowledge of security personnel and/or staff or membership about hate crime activity, suspicious behavior; emergency evacuation procedures; and similar topics that will secure the organization.

All training will require prior DCJS approval and must be within the United States, preferably within New York State. Out-of-state travel must be requested in writing and approved in writing by your assigned grants representative at DCJS. Please note these requests and approvals occur during contract development, or after contract execution. This approval is not part of the application process. Please refer to Section 4 of the questions for guidance and allowable consultant rates.

Allowable training costs include, but may not be limited to, the following:

- attendance/registration fees for training
- costs for training materials and supplies; and

- travel related costs to attend training

3. Cybersecurity Project Costs

Organizations can apply for equipment or services to improve the organization's cybersecurity. Eligible costs include, but are not limited to the following:

- Planning: Costs associated with the development of cybersecurity plans, including the contracting of consultants to identify potential vulnerabilities and develop risk mitigation plans.
- Equipment:
 - Software packages including firewalls, anti-virus applications, and malware protection.
 - Network equipment including servers.
 - Encryption software.
 - Intrusion detection systems.
 - Hardware components that provide protection against cyber threats.
- Training: Costs associated with the development and delivery of cyber awareness training to staff at the user level.
- Exercises: Costs associated with the design, development, execution, and evaluation of exercises to determine the viability of new or pre-existing cybersecurity capabilities.

C. Non-Permissible Costs

The following projects and costs are **not permissible** for award consideration. Please note, this is not an exhaustive list and DCJS reserves the right to deem a project or cost not allowable:

- A project that has previously been funded through an SCAHC grant through DHSES or DCJS, unless the new proposed project builds upon a previously funded and completed project.
- Anticipated security costs for facilities not yet built or existing.
- Security costs for facilities not being occupied by the organization.
- Personnel and fringe costs, including the hiring of security or safety personnel.
- General-use and maintenance expenditures.
- Overtime and backfill costs.
- The development of risk/vulnerability assessment models.

- Proof-of-concept initiatives.
- Food/beverage costs for attendees at in-house/local training (per diem meal costs may be allowed for training requiring travel).
- Organizational operating expenses or overhead costs (i.e. indirect costs).
- Reimbursement of pre-award costs or grant writing costs.
- Indirect costs.
- No advance payments will be allowed.

V. BEST PRACTICES AND REFERENCE MATERIALS

A. Best Practices

See Appendices [“Best Practices for Preparing an Effective Grant Application”](#) and [“Best Practice Guide for Securing Your Facility”](#) included in this RFA.

B. Reference Materials

Please see Appendices: [State and Federal Resources for Facility Security and Resources for Nonprofit Cybersecurity Projects](#) included in this RFA.

VI. EVALUATION AND SELECTION OF APPLICATIONS

Tier I Evaluation

The Tier I Evaluation assesses whether applications satisfy minimum “pass/fail” criteria for funding. All applications will be initially screened by DCJS, or other reviewers assigned by DCJS to determine their completeness using the following criteria:

- Application was received by the published deadline.
- Applicant is eligible as defined by this solicitation.
- Applicant is an eligible, **prequalified** entity in the New York Statewide Financial System, at the time of application submission. Information on prequalifying can be found in the [Appendix: SFS Prequalification Requirement](#).
- Gender-Based Violence and the Workplace Attestation
 - State Finance Law §139-m(1)(a) "By submission of this bid, each bidder and

each person signing on behalf of any bidder certifies, and in the case of a joint bid each party thereto certifies as to its own organization, under penalty of perjury, that the bidder has and has implemented a written policy addressing gender-based violence and the workplace and has provided such policy to all of its employees, directors and board members. Such policy shall, at a minimum, meet the requirements of subdivision 11 of section five hundred seventy-five of the executive law."

- To pass Tier I, the submitted application shall include:
 - Questions must be answered in the Questions tab of GMS and include a Word copy or PDF attachment in [GMS](#). Responses to questions may be reviewed to determine applicant and/or project eligibility.
 - Budget detail and justification provided in GMS Budget tab itemizing and justifying eligible expenses in support of the project.
 - Completed Project Work Plan. Standardized project work plans are included as an [Appendix](#) to this RFA and must be used and copied into the Work Plan tab of GMS. Please note that no alternative work plans will be accepted. Please enter the appropriate work plan(s) (Work Plan for Physical Security Projects and/or Work Plan for Cybersecurity Projects) as written, inserting the organization's name where indicated.
- All attachments and required documents:
 - Completed Vulnerability Assessment – *Vulnerability Self- Assessment Tool*. Complete the Assessment and upload as an attachment in the DCJS electronic grants management system, GMS. A separate Vulnerability Assessment is required for each facility where project work is proposed. If your organization has a Vulnerability Assessment that has been completed within the past year, it may be used to satisfy this requirement provided that the Assessment reflects current vulnerabilities of the facility or facilities.
 - An applicant that submits an application that includes a cybersecurity project will be required to submit a separate self-assessment describing the organization's cybersecurity capabilities and vulnerabilities. The cybersecurity self-assessment should be labeled Cybersecurity Self-Assessment and must be attached in GMS as a Word document or PDF.
 - A color, ground-level photo of the front façade of each facility included in the application close enough to show the location, but far enough away to show the immediate surroundings of the location. The photo should be labeled with the name and address of the facility and submitted as an attachment in GMS.

- Applicants must also include photos for every interior or exterior location where work is proposed to be performed. For example, if applicant is requesting to install a fence, photos must be provided showing the entire location where the fence would be installed. Photos must be labeled in a manner describing the prospective project. Post contract execution, photos of the completed project in that identified location, from the same perspective as the photos provided in the application, in a manner that clearly demonstrates the work performed, should be submitted as an attachment in GMS.

Any application that does not meet each of these conditions shall be subject to disqualification from further review. If sufficient funding is available to fund all eligible applicants that pass Tier I evaluation, DCJS reserves the right to forego further evaluation and make awards to eligible applicants contingent upon successful negotiation of budget items during contract development.

Tier II Evaluation

DCJS or other reviewers assigned by DCJS will evaluate applications that successfully pass the Tier I Evaluation. If further evaluation is deemed necessary or appropriate, a standard rating tool will be used to score responses to questions provided in the application (see *Questions* section for additional information). The maximum application score based upon responses to the questions will be 100 points. Applicants that have not previously received a SCAHC award will receive 5 points. Each response will be scored, and all scores will be totaled resulting in an overall score. The final score will be determined by averaging the reviewers' overall scores for each application. DCJS may, at its discretion, request additional information from an applicant as deemed necessary. In the event of a scoring disparity between reviewers of 15 or more points of the total available points, an additional reviewer may rate the affected application and the average of all the scores will determine the final average score of the application. In the event of a tie score among applicants, and where both applicants cannot be selected, the applicant with the highest score on the following section(s) will be given priority:

- First Tiebreaker- Applicant score on Section 2- Question 6: Vulnerability Assessment.
- Second Tiebreaker- Applicant score on Section 3- Questions 7-10: Risk Assessment.
- Third Tiebreaker- Applicant score on Section 3- Question 9.

Tier III Evaluation

The Tier III Evaluation will be conducted by designated DCJS executive staff. During the Tier III Evaluation, applicants shall be selected for funding and award amounts shall be determined through consideration of some, or all the following: Tier I eligibility review, Tier II Evaluation scoring and comments, strategic priorities, overall risk score of each application, available

funding, and best overall value to New York State.

Final award decisions will be made by DCJS in accordance with the best interests of the State. Nothing herein requires DCJS to approve funding for any applicant.

The DCJS Commissioner, or their designee, will make final decisions regarding approval and individual award amounts based on the quality of each submission, the recommendations of the reviewers, specific criteria set forth in this solicitation and, where applicable, geographic balance and comparative crime and/or risk level. Awards must be approved by the Division of the Budget and may also require Attorney General and Office of the State Comptroller approval. **All awards are subject to availability of state funds.**

VII. REQUEST FOR APPLICATIONS QUESTIONS

Important Reminders - In addition to answering the questions below and completing any other contractual requirements described in this RFA, all Applicants are required to complete and/or submit the following:

- Completed Vulnerability Assessment – See Attachment: *Vulnerability Self-Assessment Tool*. Complete the Assessment and upload as an attachment in the DCJS electronic Grants Management System, GMS. Each facility included in the application requires a separate Vulnerability Assessment. If your organization has a Vulnerability Assessment that has been completed within the past year, it may be used to satisfy this requirement provided that the Assessment reflects current vulnerabilities of each facility included in the application.
- An applicant that applies for a cybersecurity project will be required to submit a separate self-assessment describing the organization's cybersecurity capabilities and vulnerabilities. The cybersecurity self-assessment should be labeled Cybersecurity Self-Assessment and must be attached in GMS as a Word document or PDF.
- As described under Tier I Evaluation:
 - A color, ground-level photo of the front façade of each facility included in the application close enough to show the location, but far enough away to show the immediate surroundings of the location. The photo should be labeled with the name and address of the facility submitted as an attachment in GMS.
 - Photos for every interior or exterior location where work is proposed to be performed. For example, if an applicant is requesting to install a fence, photos must be provided showing the entire location where the fence would be installed. Photos must be labeled in a manner describing the prospective project.

Any application that does not meet each of the requirements detailed in this RFA **shall be subject to disqualification** from further review. See RFA Section - *Evaluation and Selection of Applicants* for additional information.

RFA Questions

Applicants must respond to the questions below within the DCJS electronic [Grants Management System \(GMS\)](#). Basic instructions can be found as an [Appendix](#) to this solicitation. A full application manual can be found here: [GMS Application Manual](#).

First, please **prepare responses to questions in a Microsoft Word Document using Arial, 11-point font and 1.5 line spacing**. Responses should then be copied and pasted to GMS under the *Questions* “Tab” of the application. Applicants are also required to attach the Microsoft Word document with responses to the questions using the *Attachments* Tab on GMS.

Responses to the questions will be scored and are the basis for Tier II Evaluation funding recommendations. Note: The aggregate scoring value assigned to all questions equals a total possible score of 100 points.

Section 1 – Questions 1-5 Organization Background & Overview (no points awarded for this section)

Please note that this contextual information is necessary to understand the reasonableness of funding requested by the applicant.

1. Identify the type of facility or facilities for which you are seeking funding as one of the following (0 Points):
 - a) House of Worship
 - b) Nonprofit School (K-_)
 - c) Nonprofit Daycare
 - d) Nonprofit Community Center
 - e) Nonprofit Cultural Museum
 - f) Nonprofit Day Camp
 - g) Nonprofit Residential Camp
 - h) Other (specify)
2. Provide your Organization’s Mission Statement (0 Points).
3. Provide a narrative to describe the nonprofit organization. Information must include, at a minimum: (0 Points)

- a) Size of Membership
 - b) Number of People Served
 - c) Community Served
 - d) Primary Use of Facility
 - e) Days & Hours of Operation
 - f) Peak Occupancy
4. Describe your organization's risk of a hate crime based on its ideology, beliefs, or mission. Include if there is a symbolic value of the site as a highly recognized national, statewide, local, or historical institution that renders the organization as a possible focus of a hate crime. (0 Points)
5. Please describe the specific location and nature of any previously funded projects. This description must provide sufficient detail (including photos of previously funded NYS or Federal projects) for DCJS to determine that the proposed project is different and distinct from those projects that were funded previously or builds upon those prior projects. By submitting the application, applicants are attesting that the proposed project does not include any items or services that have been, or will be, funded by any other funding source. (0 points)

Section 2 – Question 6 - Vulnerability Assessment (maximum 30 points)

6. Applicants must complete and upload as part of their application submission a Vulnerability Assessment. The Assessment will be scored and must be specific to the location or locations for which you are seeking funding. Each requested facility requires its own Vulnerability Assessment. Applications for a project related to cybersecurity must also include a self-assessment of the organization's current cybersecurity capabilities and vulnerabilities. If your organization has a Vulnerability Assessment that has been completed within the past year, it may be used to satisfy this requirement provided that the Assessment reflects current vulnerabilities of the facility or facilities. **The completed and attached Vulnerability Assessment and/or Cybersecurity assessment should include, at a minimum, the required information below, as well as specific recommendations for actions to mitigate the identified vulnerability:**
- a) Clearly identify the perceived threats to the facility or the organization's cyber resources. **(0-10 points)**
 - b) Clearly identify the vulnerabilities of the facility or the organization's cyber resources. **(0-10 points)**
 - c) Describe how the vulnerabilities are linked to the threats. **(0-10 points)**

Section 3 – Questions 7-11 - Risk Assessment (maximum 40 points)

7. Is there a history of hate crimes at the facility or cyber-attacks to the organization? If yes, provide a narrative for each. If you have documentation of hate crime history, such as police reports or insurance documentation, please provide them as attachment(s). **(0-10 points)**

8. Does the location of the facility contribute to the risk of a hate crime incident? If so, please describe. **(0-10 points)**

9. Describe how the proposed facility hardening equipment and/or security training will mitigate the identified threats and vulnerabilities or enhance existing security measures. For cybersecurity projects, describe how the proposed cybersecurity measures will mitigate the identified threats and vulnerabilities to the organization's cyber resources or enhance existing cybersecurity measures. **(0-10 points)**

10. Answer the following as applicable **(0-5 points)**:

a). What is the largest event attendance at the facility?

b). What is the average daily population at the facility?

11. ALL APPLICANTS ARE REQUIRED TO ENTER N/A FOR QUESTION #11. The following is provided for informational purposes and the applicable points will be applied by DCJS:

Risk demographics – Applications will receive the following points based on the information provided in [Appendix: Reported Hate Crime Incidents for County](#)

a) Reported Hate Crime Incidents for County **(0-5 points)**

Section 4 – Questions 12-14 - Budget Details and Workplan (maximum 25 points)

12. Operating Budget Detail and Justification **(0-15 points)**

a) Using the Budget Detail Worksheet and Budget Narrative sheet as a guide, enter the **allowable** costs in the operating budget directly into the Budget "Tab" of the GMS application. Prepare a line-item budget, including justification, by appropriate category of expense (i.e., Equipment, etc.).

- For this RFA, items requiring physical installation or any modification to physical structures should be placed in the Alterations and Renovations category. This includes but is not limited to surveillance cameras, lighting, fencing, door/window locks or upgrades, and access control systems.
- Personnel positions, operating costs, and indirect costs are not

allowable expenses.

- Budgets should reflect total projected costs for a 24-month contract period and be limited to eligible costs as described in the RFA. Operating budgets must not exceed the applicant's maximum eligible award amount of \$250,000 per application.
- b) A detailed cost breakdown for each item must be provided. A quote or an explanation describing the basis of the cost estimate for each budget line should be used to support the reasonableness of the estimate included in the application. Please note that this estimate does not satisfy the contractual procurement requirements. Please describe how this project is separate and apart or enhancing any previously state or federally funded project.
- c) If a paid trainer is to deliver training, the cost should be listed in the budget category as "Consultant Services." Training materials should be listed under the "Supplies" budget category.
- d) Consultant Services: All consultant services must be obtained in a manner that provides for fair and open competition. Please note:
- The rate for a consultant should not exceed \$650 for an eight-hour day (not including travel and subsistence costs).
 - A rate exceeding \$650 per eight-hour day requires prior written approval from DCJS and may be approved on a case-by-case basis where adequate justification is provided, and expenses are reasonable and allowable.
 - A grant award recipient who proposes to obtain consultant services from a vendor without competitive bidding will be required to obtain the prior written approval of DCJS. The request for approval must be in writing and set forth, at a minimum, a detailed justification for selection and basis upon which the price was determined to be reasonable. Further, such consultant services must be in accordance with the guidelines, bulletins, and regulations of the NYS Office of the State Comptroller and the State Procurement Council.
 - Not-for-Profit entities and not-for-profit subgrantees and/or subcontractors that are receiving an award of \$100,000 or greater are required to complete a Vendor Responsibility Questionnaire.
- e) The detailed budget for the grant period must be complete and provide sufficient detail to justify expenditures. It must also be reasonable and appropriate, as determined by DCJS, and directly tied to the Work Plan and vulnerabilities identified in the Vulnerability Assessment. 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.

13. Please detail how you plan to procure any vendors, contractors, equipment, etc. for your proposed project(s). Please illustrate how this adheres to the [Procurement Requirements – Guidelines – Vendor Selection](#) section of this RFA. Please note, if an application indicates a Single or Sole source procurement and receives an award this **does not** imply DCJS' approval of the Single or Sole source. Approval of a Single or Sole source will need to be obtained post award during the contract process. **(0-10 points)**
14. Complete the project work plan in the Work Plan tab of GMS using the [Appendix: Standardized Project Work Plan](#) (*Physical Security Projects and/or Cybersecurity Projects*). (0 points)

Section 5 – Question 15- Project Eligibility (maximum 5 points)

15. Has your organization previously received an SCAHC grant award from DHSES or DCJS? Enter Yes or No to this question. **(5 points for NO)**

VIII. NOTIFICATION OF AWARDS

Applicants approved for funding will be notified in writing by DCJS to the signatory email address provided in GMS. The terms of the final contract agreement are subject to negotiation between DCJS and the grantee.

If DCJS and a successful award recipient cannot agree to contract terms within ninety days of notification of selection for award, DCJS reserves the right to rescind the award and redistribute the funds.

For those not approved to receive funding awards, notifications will be sent to the contact email address provided in the Grants Management System.

Pursuant to §163(9) (c) of the State Finance Law, any non-awarded applicant may request a debriefing regarding the reasons that the application submitted by the applicant was not selected for award. Requests for a debriefing must be made within fifteen (15) calendar days of written notification by DCJS that the application(s) submitted by the applicant was not selected for award.

An unsuccessful applicant's written request for a debriefing must include specific questions that the applicant wishes to be addressed. Questions must be submitted to the DCJS funding mailbox at dcjsfunding@dcjs.ny.gov with the following in the subject line: **Request for Debriefing (Securing Communities Against Hate Crimes)**. The debriefing shall be scheduled to occur within 30 business days of receipt of request by DCJS or as soon after

that time as feasible.

The method for the debriefing will be based upon mutual agreement by all parties and can be conducted via telephone, webinar, videoconference or if necessary, in-person or any combination thereof.

IX. REPORTING REQUIREMENTS

Standard reporting requirements are provided below and may be changed depending on applicability:

GMS Progress Reporting

All grantees will be required to submit **annual** progress reports via GMS that describe annual performance and activities in support of the project work plan entered in GMS. These annual reports must be submitted until the final project report is completed.

Quarterly Fiscal Reports

All grantees may submit quarterly fiscal reports and claims for payment.

Reporting Due Dates:

GMS Progress Reports (if applicable), Case-specific Reports (if applicable) and Fiscal Claims for Payment are due to DCJS by the dates indicated, or as otherwise stated in the contract:

<u>Calendar Quarter</u>	<u>Due Date</u>
January 1 - March 31	April 30
April 1 - June 30	July 31
July 1 - September 30	October 31
October 1 - December 31	January 31

X. ADMINISTRATION OF CONTRACTS

DCJS will negotiate and develop a contract with each successful applicant. If DCJS and the successful applicant cannot agree to contract terms within ninety days of notification of awards, DCJS reserves the right to rescind the award, and to redistribute the funds.

Contract Approval

A grant contract may be subject to approval by the NYS Office of the Attorney General (AG) and the Office of the State Comptroller (OSC) before funding may be disbursed. For contracts subject to the approval of the Attorney General and the Comptroller of the State of New York, the contract shall be of no force and effect until said approval has been received and indicated thereon.

Contract Term

DCJS will enter into a contract period as noted in this solicitation. DCJS reserves the right to modify the contract term in the best interests of the State.

Contract Activities

All activities must have prior approval from DCJS and meet the guidelines established by the State of New York.

Contract Changes

Contracts resulting from this solicitation may be executed, increased, terminated, renewed, decreased, extended, amended, or renegotiated for any reason at the discretion of DCJS or designee because of contractual performance, changes in project conditions, or as otherwise may be in the best interests of New York State.

Records

The Grantee shall establish and maintain complete and accurate books, records, documents, accounts and other evidence directly pertinent to performance under this contract (hereinafter, collectively, the "Records"). The Records must be kept for the balance of the calendar year in which they were made and for six (6) additional years thereafter. The State Comptroller, the Attorney General and any other person or entity authorized to conduct an examination, as well as the agency or agencies involved in this contract, shall have access to the Records during normal business hours at an office of the Grantee within the State of New York or, if no such office is available, at a mutually agreeable and reasonable venue within the State, for the term specified above for the purposes of inspection, auditing and copying. The State shall take reasonable steps to protect from public disclosure any of the Records which are exempt from disclosure under Section 87 of the Public Officers Law (the "Statute") provided that: (i) the Grantee shall timely inform an appropriate State official, in writing, that said records should not be disclosed; and (ii) said records shall be sufficiently identified; and (iii) designation of said records as exempt under the Statute is reasonable. Nothing contained herein shall diminish, or in any way adversely affect, the State's right to discovery in any pending or future litigation.

Liability

Nothing in the contract between DCJS and the grantee shall impose liability on the State of

New York for injury or damages incurred during the performance of approved grant activities or caused by the use of equipment purchased with grant funds.

Payments

Payments to reimburse project expenses will be made pursuant to a schedule specified in the contract between the State of New York and the grant award recipient. Where applicable, performance-based expenses will be reimbursed in compliance with the contract milestone performance and costs budget and the project work plan. Payment for invoices submitted by the contractor shall only be rendered electronically unless payment by paper check is expressly authorized by the Commissioner or their designee, in the Commissioner's sole discretion, due to extenuating circumstances. Such electronic payment shall be made in accordance with ordinary State procedures and practices. The contractor shall comply with the State Comptroller's procedures to authorize electronic payments. Authorization forms are available at the State Comptroller's [website](#), or by email at epayments@osc.ny.us. Contractor acknowledges that it will not receive payment on any invoices submitted under this contract if it does not comply with the State Comptroller's electronic payment procedures, except where the Commissioner has expressly authorized payment by paper check as set forth above.

To enroll in e-Payments:

1. Log in to the [Vendor Self-Service Portal](#).
2. Select the "Enroll in e-Payments (Direct Deposit)" link.
3. Follow the prompts to complete your enrollment.

Don't have an account? [Enroll in the Vendor Self-Service Portal](#)

Update or add additional bank accounts.

See the section *Update or Add Locations* at [Update Vendor Information and Access](#).

For assistance, email ePayments@osc.ny.us

Reports

The grantee shall submit all reports to DCJS in a format and time frame as specified in the contract. Progress reports shall include a description of the grantee's efforts undertaken during the reporting period and the current status of the project. The progress reports of the grantee's activities under this contract must be submitted electronically as directed by DCJS. Independent of any reporting schedule, all grantees will be required to inform DCJS of any project issues that are significantly impacting the project performance. Any project funded under this solicitation must comply with the requirements established by DCJS. The grantee agrees to submit any other reports considered relevant by DCJS.

Performance Review

The grantee's performance in all areas mentioned above, in addition to the services contracted for, will be monitored periodically by DCJS or its designee agency, and may take the form of site visits, project file review, written and telephone communication, or any other methods deemed necessary by DCJS to ascertain the quality and quantity of grantee activities.


Disposition of Allocations

DCJS reserves the right to reject applications, deny awards, or defer applications for future consideration based on insufficient information in the application, lack of accompanying documentation, the inappropriateness of the project proposed, an organizational history of unsuccessful projects of a similar nature, or a history of contract non-compliance.

Revocation of Funds

Funds awarded to an applicant who does not initiate an approved project within 90 calendar days of the contract start date may be revoked and redistributed at the discretion of the Executive Deputy Commissioner of the DCJS or designee.

Encouraging Use of New York State Businesses in Contract Performance

New York State businesses have a substantial presence in State contracts and strongly contribute to the economies of the State and the nation. In recognition of their economic activity and leadership in doing business in New York State, applicants for this solicitation are strongly encouraged and expected to consider New York State businesses in the fulfillment of the requirements of the contract(s) resulting from this solicitation. Such partnering with New York State businesses may be as subcontractors, suppliers, protégés or other supporting roles. 

Use of Service-Disabled Veteran-owned Business Enterprises in Contract Performance

Article 17-B of the Executive Law enacted in 2014 acknowledges that Service-Disabled Veteran-Owned Businesses (SDVOBs) strongly contribute to the economies of the State and the nation. As defenders of our nation and in recognition of their economic activity in doing business in New York State, bidders/proposers for this contract for commodities, services or technology is strongly encouraged and expected to consider SDVOBs in the fulfillment of the requirements of the contract. Such partnering may be as subcontractors, suppliers, protégés or other supporting roles. SDVOBs can be readily identified on the [directory of certified businesses](#).

Bidders/applicants need to be aware that all authorized users of this contract will be strongly encouraged to the maximum extent practical and consistent with legal requirements of the State Finance Law and the Executive Law to use responsible and responsive SDVOBs in purchasing and utilizing commodities, services and technology that are of equal quality and functionality to those that may be obtained from non-SDVOBs. Furthermore, bidders/applicants are reminded that they must continue to utilize small, minority and women-

owned businesses consistent with current State law. Utilizing SDVOBs in State contracts will help create more private sector jobs, rebuild New York State's infrastructure, and maximize economic activity to the mutual benefit of the contractor and its SDVOB partners. SDVOBs will promote the contractor's optimal performance under the contract, thereby fully benefiting the public sector projects that are supported by associated public procurements.

Public procurements can drive and improve the State's economic engine through promotion of the use of SDVOBs by its contractors. The State, therefore, expects bidders/applicants to provide maximum assistance to SDVOBs in their contract performance. The potential participation by all kinds of SDVOBs will deliver great value to the State and its taxpayers.

Bidders/proposers can demonstrate their commitment to the use of SDVOBs by responding to the questions on the form located [here](#) and attach the completed form, along with your Application, to the NYS Division of Criminal Justice Services' Grants Management System (GMS). There are no points attributable to this component of the application.

Standard Contract Provisions

Any contracts negotiated as a result of this solicitation will be subject to the provisions of the State of New York Contract for Grants, including the Appendix A - NYS Standard Term and Conditions, Agency Specific Terms and Conditions, Program Specific Terms and conditions, and other standard clauses for all New York State grant contracts with DCJS. Applicable contract appendices and attachments are available on the [DCJS website](#).

Minority and Women-Owned Business Enterprises (M/WBE) and Equal Employment Opportunity (EEO) Requirements

DCJS recognizes its obligation under New York State Executive Law Article 15-A to promote opportunities for the participation of certified minority- and women-owned business enterprises (M/WBEs), as well as the employment of minority group members and women in the performance of DCJS contracts.

Executive Law Article 15-A: "State contract" shall mean: (a) a written agreement or purchase order instrument, providing for a total expenditure in excess of twenty-five thousand dollars, whereby a contracting agency is committed to expend or does expend funds in return for labor, services including but not limited to legal, financial and other professional services, supplies, equipment, materials or any combination of the foregoing, to be performed for, on behalf of, or rendered or furnished to the contracting agency; (b) a written agreement in excess of one hundred thousand dollars whereby a contracting agency is committed to expend or does expend funds for the acquisition, construction, demolition, replacement, major repair or renovation of real property and improvements thereon; and (c) a written agreement in excess of one hundred thousand dollars whereby the owner of a state assisted housing project is committed to expend or does expend funds for the acquisition, construction, demolition, replacement, major repair or renovation of real property and

improvements thereon for such project.”

As such, all contracts in excess of \$100,000 and some contracts in excess of \$25,000 require grant recipients to document good faith efforts to provide meaningful participation by M/WBEs as subcontractors or suppliers in the performance of grant contracts.

Accordingly, applicants requesting in excess of \$25,000 must be prepared to submit a Local Assistance M/WBE Subcontractor/Supplier Utilization Proposal Form (DCJS-3301), and a Local Assistance M/WBE NPS Discretionary Budget Determination Worksheet (DCJS-3309). All forms are located at the [DCJS website](#). For contracts between \$25,000 and \$100,000, DCJS staff will determine whether M/WBE forms are required based on the nature of the project and items/services to be funded.

DCJS will review the submitted Local Assistance M/WBE Subcontractor/Supplier Utilization Proposal Form, Local Assistance M/WBE NPS Discretionary Budget Determination Worksheet, and Minority and Women-Owned Business Enterprises and Equal Employment Opportunity Policy Statement and advise the applicant of DCJS' acceptance once an award determination is made. There are no points attributable to this component of the application.

Sexual Harassment Prevention Certification

As of January 1, 2019, bidders on procurements subject to competitive bidding in New York State, are required to submit a certification with every bid that states they have a policy addressing sexual harassment prevention and that they provide sexual harassment training to all employees on an annual basis. Pursuant to State Finance Law §139-l, bidders responding to a competitively bid Request for Applications (RFAs) must certify that by submission of their bid, each bidder and each person signing on behalf of any bidder certifies, and in the case of a joint bid each party thereto certifies its own organization, under penalty of perjury, that the bidder has implemented a written policy addressing sexual harassment prevention in the workplace and provides annual sexual harassment prevention training to all of its employees. Such policy shall, at a minimum, meet the requirements of section two hundred one-g of the labor law. Bidders that do not certify will not be considered for award; provided however, that if the bidder cannot make the certification, the bidder provides a signed statement with their bid detailing the reasons why the certification cannot be made.

In addition to requiring this certification for competitively bid RFAs, DCJS has included this requirement for all grantees receiving funds from DCJS. Grantees must provide certification that they have implemented a written policy addressing sexual harassment prevention in the workplace and that they provide annual sexual harassment prevention training to all their employees.

Therefore, all applicants to this RFA must complete the certification provided on the DCJS website and submit the completed [certification](#) as an attachment to the application in GMS.

Vendor Responsibility

Not-for-Profit entities and not-for-profit subgrantees and/or subcontractors that are receiving an award of \$100,000 or greater are required to complete a Vendor Responsibility Questionnaire. The questionnaire and additional information are available on the NYS Office of [State Comptroller website](#). The Vendor Responsibility Questionnaire must be certified or updated within the last six months to be considered current for contract approval. DCJS recommends creating an account in the New York State Vendor Responsibility System to complete and certify the Questionnaire online.

Charities Registration

Not-for-Profit entities must also ensure that their filing requirements are up-to-date with the Charities Bureau of the NYS Attorney General's Office. Further information on the registration requirements may be obtained at the [Attorney General's website](#).

Organizations that are exempt from this requirement must provide a letter on their respective letterhead attesting that they are exempt and explaining why.

XI. APPLICATION SUBMISSION AND REQUIREMENTS

A. Specific Instructions

Applicants may submit one (1) application that will include all proposed projects. Applications must be submitted using the DCJS Grants Management System (GMS). Prior recipients of a Division of Homeland Security and Emergency Services (DHSES) or DCJS Securing Communities Against Hate Crimes award may not apply to fund the same project under this RFA, but may fund a new, different project at the same facility, or a new project that builds upon the previous one.

B. Grants Management System (GMS)

Applications must be submitted to DCJS using the [Grants Management System](#) (GMS). First time GMS users should download the GMS Application Manual [here](#). If you need assistance with accessing and using GMS, please contact the DCJS Office of Program Development and Funding (OPDF) GMS Help Desk at (518) 457-9787. **The DCJS GMS Help Desk is available Monday through Friday between the hours of 9:00 am and 5:00 pm. However, applicants should note specific RFA submission deadlines.**

The following information is specific to this solicitation. For general guidance and GMS Helpful Hints see [Appendix: Grants Management System \(GMS\) Instructions and Helpful Hints](#).

Submitting an Application in GMS

To submit a new application in GMS, log on to the system and click on “Project.” Click the “New” button at the top of the project grid. This will take you to a screen that says, “Select a Program Office.” Using the drop-down box, find and select the name of the program **Securing Communities Against Hate Crimes**. Click “Create Project.” Your application will now be ready to complete.

Completing the Application

Applicants must complete the GMS registration as well as the registration and/or prequalification on the NYS Financial System early, where applicable, to avoid any concerns with these automated systems. NYS Financial System prequalification and GMS signatory registration **must** be completed prior to the final submission of an application. Each application will consist of the following components that must be completed using GMS:

- Participant name(s): primary contact, fiscal contact, contract signatory.
- Contact information for all participating agencies or organizations.
- Answers to project specific questions.
- Project Budget.
- Project Work Plan.
- Any required attachments indicated in this RFA and noted below in the checklist.

When all the above requirements and GMS Application components are completed, click the “**Submit**” button. GMS will review the application for completeness. If any fields are missing, a report will display what remains to be completed. Once all fields are complete and you submit successfully, GMS will display a screen that states, “*Your application has been submitted.*”

Please note, this only indicates that your application has met the minimum system requirements. It does not guarantee that all required documents have been included or are complete/sufficient.

XII. APPLICATION CHECKLIST

- Complete SFS Prequalification Requirements – See [Appendix: SFS Prequalification Requirements](#).
- All Applicants: Complete all DCJS Grants Management System (GMS) Registration Requirements – See [Appendix: DCJS Grants Management System \(GMS\) Instructions and Helpful Hints](#).
- Complete all necessary contractual requirements as described in [Section X:](#)

[Administration of Contracts.](#)

- Complete all Tier I and Tier II evaluation requirements.
- Answer Project Narrative Questions in *QUESTIONS* TAB in GMS **AND** also attach the answers in a Word Document to GMS.
- Complete BUDGET TAB on GMS by entering the line-item Operating Budget with justifications.
- Complete project WORK PLAN TAB in GMS by copying and entering the content of [Appendix: Standardized Project Work Plan](#) (*Physical Security and/or Cybersecurity*).
- Attach in GMS a completed facility Vulnerability Assessment (Attachment: *Vulnerability Self-Assessment Tool*) for each facility included in the application.
- An applicant that submits an application that includes a cybersecurity project will be required to submit a separate self-assessment describing the organization's cybersecurity capabilities and vulnerabilities. The cybersecurity self-assessment should be labeled Cybersecurity Self-Assessment and must be attached in GMS as a Word document or PDF.
- A color, ground-level photo of the front façade of each facility included in the application—close enough to show the location, but far enough away to show the immediate surroundings of the location for each application. The photo should be labeled with the name and address of the facility submitted as an attachment in GMS. Applicants must include a photo for each facility where they are proposing security enhancements.
- Applicants must also include photos for every interior or exterior location where work is proposed to be performed. For example, if applicant is requesting to install a fence, photos must be provided showing the entire location where the fence would be installed. Photos must be labeled in a manner describing the prospective project.

Appendix : SFS PREQUALIFICATION REQUIREMENT

Pre-Qualification

Pursuant to the New York State Division of Budget Bulletin H-1032, dated June 7, 2013 and revised January 19, 2025 , New York State has instituted key reform initiatives to the grant contract process, which require not-for-profits to register and complete the Vendor Prequalification process for applications to be evaluated. Information on these initiatives can be found on the [Grants Management website](#).

Not-for-profit organizations **must** prequalify to do business with New York State agencies **before** they can compete for State grants. To become prequalified, a not-for-profit must first [register](#) with SFS. Once registered, not-for-profits must complete an online Prequalification application. This includes completing a series of forms by answering basic questions regarding the organization and uploading key organizational documents. Grant applications received from not-for-profit applicants that are not Prequalified in the SFS on the application due date and time will not be evaluated. Such applications will be disqualified from further consideration. **Vendors are strongly encouraged to begin this process as soon as possible to participate in this opportunity.**

Required Forms and Documents

Forms that must be completed for prequalification include:

- Organizational Capacity
- Organizational Compliance
- Organizational Integrity
- Service Descriptors
- Service Capacity

Documents that must be uploaded include:

- Certificate of Incorporation or equivalent document
- IRS 501(c) determination letter
- IRS 990
- Audit/Reviews and Findings
- CHAR500 or CHAR410
- Board of Directors Profile
- Senior Leadership Resumes
- Corporate By-Laws

Three of a not-for-profit's essential financial documents - the IRS990, Financial Statement and Charities Bureau filing - expire on an annual basis. A not-for-profit must upload current versions of

these documents and submit their updated Document Vault for review and approval **each year** to maintain prequalification. Not-for-profits are provided a full 10.5 months from the end of their fiscal year to provide a current IRS990 or Financial Statement without the interim requirement of uploading extension requests.

Specific questions about the prequalification process should be referred to your agency representative or to the Grants Reform Team at grantsreform@its.ny.gov.

Disclaimer: *New York State reserves 5-10 business days from the receipt of complete Prequalification applications to conduct its review. If supplementary information or updates are required, review times will be longer. Due to the length of time this process could take to complete, it is advised that not-for-profits Prequalify as soon as possible. Failure to successfully complete the Prequalification process early enough will result in a grant application being disqualified.*

Vendors are strongly encouraged to begin this process as soon as possible to participate in this opportunity.

Appendix: DCJS GRANTS MANAGEMENT SYSTEM (GMS) INSTRUCTIONS AND HELPFUL HINTS - [See RFA for additional specific GMS directions.](#)

First time [GMS](#) users should download the GMS Application Manual [here](#). Persons familiar with GMS can use the following simplified guidelines:

If any company or individual is acting on behalf of an applicant/grantee, GMS Attestation letters must be submitted to the DCJS GMS Help Desk. Further information can be found on our [Applicant and Grantee Resources website](#).

Getting Started: Sign on to GMS.

Click "Project" to go to project grid. Click the "New" button at the top of the project grid. This will take you to a screen that says "Select a Program Office" in a drop-down box format. Find and highlight "Securing Communities Against Hate Crimes," then click "Create Project."

This begins your application. You may work on the application, save and return to it at a later time, except as noted below. **Note that GMS will time out after 30 minutes of inactivity.** That means that you should save your work frequently. Each save re-sets the timer.

In the newly created project complete the following Tabs which are listed across the top of the screen:

General - Complete the text screens and press save.

Participants/Contacts - Complete the text screens and press save.

Click on "Add Participant" and in the search prompt that appears type in your agency name. This should take you to a list, find your agency, and click in the blue section of your agency name. This will prompt a drop-down list that defaults to "Grantee." Click "Add." If there will be a separate Implementing Agency, repeat the process, choosing "Implementing Agency" as the Participant Type. In the event your agency is not listed, click the "New" button to add your agency to our database. Please complete all required information on the screen, including the Employer Identification Number (EIN) before you SAVE the entry. GMS will only allow one attempt then locks the entry to edits. Should you still need additional information added to the Participant record, please call GMS Help at (518) 457-9787.

Scroll to the bottom of the screen to add contact information. Click on "Add Contact" and in the search prompt that appears type in the last name of the person to be added. This should take you to a list. Find the person to be added and click in the blue section of the name. This will prompt a drop-down list that defaults to "Primary." Ensure you do this until you have added a minimum of three contacts: Primary, Signatory and Fiscal. If the contact you are attempting to add does not appear in a search, click the "New Contact" button to add the contact to our database.

Note: If the signatory you attempt to add is not eSignature registered, you will get an error message and will not be allowed to add that person at that time. You will NOT be able to submit the application without a signatory attached. Please refer [here](#) to add a signatory for your agency.

Budget - See RFA for additional specific instructions.

Work Plan - In the GMS Work Plan Tab, enter the Project Goal, Objectives, Tasks and Performance Measures provided in the Standard Work Plan within this solicitation, unless otherwise instructed within the solicitation. Please note, the standardized work plans for physical security projects and cybersecurity projects are different. Please use the appropriate plan(s) for your project.

- ✓ Fill in the "Project Goal" text box and click "Save."
- ✓ Click "Create New Objective" and fill in the text box and click "Save."
- ✓ Click "Add Task to this Objective" and fill in the text box and click "Save."
- ✓ Click "Add Performance Measure to this Task" and fill in the text box and click "Save."

Questions-

Answer all required project narrative and budget information questions.

Hint: Answers should be developed in Word. GMS will time out after 30 minutes and unsaved material will be lost. Cutting and pasting from a Word document will prevent the loss of any work.

Attachments -

Click on "Attachment," and upload the required attachments for this solicitation. Note: Follow the instructions in the GMS User's Manual for Attachments; also, see screen instructions for accepted file types and advice on file names.

Remember: Failure to submit required documents will be considered the same as failure to meet the deadline for application submission. This may result in a non-award due to the application being untimely.

When all requirements are completed, click the "Submit" button. If any fields are missing, a report will display what remains to be completed. Once all fields are complete and the application is submitted, GMS will display a screen that says, "*Your application has been submitted.*" Please note, this is simply an indication that minimum system requirements have been met for submission. It does not suggest that all required documents have been included or are complete/sufficient. In addition, GMS will send an email notification to the Signatory listed on the application to make them aware an application has been submitted on your organization's behalf.

Appendix: *BEST PRACTICES FOR PREPARING AN EFFECTIVE GRANT APPLICATION*

What to do when you have received the Request for Applications (RFA):

It is important to start early in preparing your application, highlighting deadlines and/or tasks that must be completed as part of the application process.

Review all plans, strategies, policies and documents related to the grant you are applying for to ensure you can appropriately address the goals and objectives pertaining to the nature of the grant opportunity.

What to do when you are completing the application:

Ensure that the proposed budget is realistic, reasonable, and articulate how your budget will address the objectives of the grant opportunity, as well as how it will **mitigate the threat/vulnerabilities** that have been identified in the Vulnerability Assessment.

Review and evaluate the scoring criteria. Pay close attention to the sections that are weighted the most first as they have a greater impact on your overall score.

What to do prior to submitting your application:

Make sure that you have completed all the required sections of the application and attached all the required documents in GMS. Applicants are strongly recommended to share their completed applications with a colleague to ensure that the application is clearly written, complete, and addresses all the objectives of the grant opportunity.

Appendix: *BEST PRACTICE GUIDE FOR SECURING YOUR FACILITY*

This information provides examples of best practices to secure your facility from man-made threats which include, but are not limited to, an Active Shooter, Improvised Explosive Device (IED), Vehicle- Ramming, or use of an Edged Weapon.

The information is broken into two sections. Section one is organized into five focus areas that demonstrate how basic security measures can be considered and implemented. *Basic* actions, or those that require little to no costs, primarily involve coordination among the facility staff and local first responders. Section two provides a table of *Intermediate* or low-cost actions that provide immediate benefits, and *Advanced* actions that cost more up-front and can be implemented over time.

The security measures mentioned in this document are not exhaustive lists, rather, intended to provide a starting point or building blocks for applying protective measures to enhance security.

***Please Note:** Some actions identified in this document are not allowable expenditures under the Securing Communities Against Hate Crimes Grant Program. Please ensure all budget items in your application are allowable according to the guidelines of this grant opportunity.

SECTION 1. BASIC ACTIONS

PERIMETER AND INTERIOR SECURITY MEASURES - Physical features or administrative actions that protect the facility and those inside it from the threat occurring.

- Access into the facility is controlled.
- Internal and external doors have functioning locks.
- All visitors are required to sign-in, receive a pass, and even be escorted if appropriate.
- All doors and rooms/windows are uniformly labeled on both sides to aid in emergency response.
- Evacuation routes are posted next to all doors.
- Lists of prohibited items (i.e., weapons) are posted at points of entry.
- Rooms that can provide safe haven have been identified (rooms with "hard corners" or minimal doors and windows). These rooms should be locked easily.
- Interior and exterior lighting is adequate to provide a safe environment.
- Landscaping (i.e., trees, bushes) is maintained to minimize areas to hide or obstruct views.
- Bus and other drop-off zones take place in areas away from parking areas and roadways.
- Speedbumps and other techniques are used to slow vehicular movements on the grounds.
- Grounds and parking lots are fenced in where appropriate.

SURVEILLANCE AND EMERGENCY RESPONSE CAPABILITIES - Leadership and culture that aid in the response to an incident on-site.

- Establish a Facility Security Committee that meets regularly.
- Promote a Security-Focused Culture.

- Staff participate in security by monitoring their surroundings and regularly inspecting hallways, classrooms and stairwells for suspicious items and behavior.
- Use phone trees during emergencies to maintain an informed, well-connected workforce, membership, and community.

RELATIONSHIPS WITH KEY PARTNERS - Consistent engagement with local law enforcement, fire, EMS, emergency managers, and other public safety professionals.

- There is regular engagement with first responders through informal (i.e., "coffee break" or meet-and-greet) and formal (i.e., patrol) settings.
- Phone numbers for facility leadership are shared with local first responders.
- Emergency phone numbers are posted in offices and common areas.
- A Knox Box is installed near the main entrance to aid in response.
- Lists of key events (i.e., holidays, large or notable events) are shared with local law enforcement.
- Incidents that occur at the facility are reported to local law enforcement.
- Local law enforcement is involved in the creation and testing of active shooter preparedness, bomb threat, and vehicle-ramming response plans.
- All areas of the grounds and interior of the facility are accessible by emergency personnel.
- Local law enforcement has been engaged in discussions related to measures to control traffic during large events or services.

TRAINING/AWARENESS - Educating and training staff and visitors on security and preparedness.

- Fire, evacuation, and other emergency drills are conducted regularly.
- Staff and visitors, where appropriate, are trained on identifying suspicious activities and familiar with the See Something Say Something program.
- Train staff and provide checklists of what information to document during a bomb threat.
- Staff are trained on the *Run, Hide, Fight* method.
- Staff are trained to provide first aid, including CPR with AED and Stop the Bleed.
- Train staff on identifying alternate evacuation routes; and establish muster points in hardened areas.
- Staff are trained on identifying suspicious mail and packages and creating vehicle-ramming response plans.

POLICIES AND PROCEDURES - Emergency plans that guide staff and visitors in preventing and responding to an incident on-site.

- A policy and list of prohibited items are disseminated to staff and posted on the

organization's website. Social and other media can also be used in advance of events and large gatherings.

- Emergency plans are reviewed regularly and communicated to staff, visitors and local first responders.
- There is a clear procedure for reporting incidents to leadership and/or local law enforcement.
- There are procedures for safe mail/package handling.
- An active shooter preparedness plan is created, which discusses the *Run, Hide, Fight* method, where designated safe rooms are located, how to respond when law enforcement arrives, and indicates how to report incidents.
- A bomb threat plan is created, detailing evacuation procedures and maps, what key information to capture in the event of a bomb threat, and how to report incidents.
- A vehicle-ramming prevention and response plan is created, detailing all potential evacuation procedures and maps, identifying hardened areas inside and outside of the facility to muster, and notice of where and how to submit incident report.

SECTION 2. INTERMEDIATE AND ADVANCED ACTIONS

Intermediate or "Low-Cost Actions"	Advanced or "Long-Term" Actions
Provide clear transitions from public to semi-private and private space.	Harden entranceways and ground floor windows; maintain and/or update locks and hardware.
Develop a strategy to utilize security guards and a contracting mechanism.	Install a facility-wide public address (PA) system and consider incorporating panic or duress buttons in locations where staff interact with visitors.
Update or add signage to restrict access, designate entrances and exit-only doors, label visitor-only parking, etc.	Install electronic access control systems.
Ensure that activities such as bus loading and visitor drop-offs take place in safe locations.	Install Closed-Circuit Television (CCTV) cameras that can record for at least 30 days.
Separate employee and visitor access points.	Hire security staff and contract for K9 sweeps during large events.
Create template messages for emergencies that can be disseminated to staff, volunteers, parents, and/or the media following an incident.	Purchase screening equipment and conduct screening and/or bag checks during events to detect suspicious items.

Use trash receptacles that can be easily checked for suspicious objects, such as wire-style cans with transparent bags and locate them away from entrance and egress points to limit places that can be used to conceal items.

Implement vehicle barriers or bollards to prevent vehicular access to pedestrian walkways, courtyards, playing fields, and other key locations.

Establish Go Bags with supplies you may need in an emergency. They should be kept in different locations at your venue and at an evacuation site.

Use self-locking doors that are compliant with fire codes but provide safe havens.

Appendix: STATE AND FEDERAL RESOURCES FOR FACILITY SECURITY

State Resources:

- [Safeguard New York](#) - Safeguard New York is an outreach initiative designed to educate individuals, community groups and other public and private sector organizations on how to recognize and report suspicious activity. Click the link for more information.

Safeguard New York promotes the "See Something, Say Something" campaign, encouraging New Yorkers to get involved in the fight against terrorism. Please remain alert and report any suspicious activities. State residents should call the toll-free statewide Terrorism Tips Hotline:

1-866-SAFENYS (1-866-723-3697)

- [Educational Resources](#) - The publications and media located at the preceding link are offered by the NYS Office of Counter Terrorism (OCT) free-of-charge by downloading from the site. Permission is granted to reproduce publications for the intent of educational purposes only. Select materials are also available to order for mail delivery, using the [order form](#)
- [480 Seconds- Surviving an Active Shooter](#) - This active shooter training details how to prepare and respond to an active shooter incident using the Run, Hide, Fight method. Additional tips are provided, like how to respond when law enforcement arrives on the scene.
- [New York State Anti-Hate Crime Resource Guide](#)
- **Information and training requests:**
 - **General Inquiries**
OCT@dhses.ny.gov
 - **Outreach**
SafeguardNY@dhses.ny.gov
 - **Intelligence Liaison Officer (ILO) Training**
ILO@dhses.ny.gov

Federal Resources:

- [Physical Security](#) – The Department of Homeland Security (DHS) recognizes that communities are the first line of defense in keeping the public safe. This program

provides free resources for the public on securing facilities and gatherings and provides tools and resources for the community to use.

- [Active Shooter Preparedness](#) - Active Shooter resources on this website are available to enhance preparedness efforts for the whole community.
- [Bombing Prevention](#) - The Office for Bombing Prevention leads DHS's efforts to counter the use of explosives against the public and private sectors. Resources available include a guide on what to do during a bomb threat, awareness training, and resources for information sharing.
- [Guide for Developing High- Quality Emergency Operations Plans for Houses of Worship](#) - FEMA's guide provides in-depth information on how to plan for security at your facility, while utilizing the prevent, protect, mitigate, respond, and recover principles.
- [Faith Based and Volunteer Partnership Resources](#) - Training and planning exercises may enhance the disaster preparedness – and response and recovery capabilities and capacity – of the voluntary, faith-based, and community partner organizations, staff and volunteers.

Additional Federal Resources

- The Department of Justice runs the [Community Relations Service](#), who serve communities in conflict through mediation and other resolution tactics and support programs that combat hate crimes.
- The Disability.gov resource page provides information on promoting inclusive workspaces. The [Emergency Preparedness](#) section provides numerous resources that support inclusive security planning
- The Federal Bureau of Investigation's Office of Partnerships has a [resource page](#) dedicated to Active Shooter Incidents, with an overview of training opportunities and videos and bulletins or guides detailing these incidents.
- The United States Fire Administration runs the [Preventing Arson at Houses of Worship](#) outreach program, designed to share information and raise awareness of arson and provide strategies to combat those problems at the community level:
- [FEMA Emergency Management Institute](#) provides free courses for all individuals, to enhance preparedness efforts and knowledge.
 - Sample of courses:
 - [Active Shooter: What You Can Do \(IS-907\)](#)
 - [Community Preparedness: Implementing Simple Activities for](#)

[Everyone \(IS-909\)](#)

- [Preparing for Mass Casualty Incidents: A Guide for Schools, Higher Education, and Houses of Worship \(IS-360\)](#)

Appendix: RESOURCES FOR NONPROFIT CYBERSECURITY PROJECTS

- The [National Council of Nonprofits](#) provides basic information and links to additional resources for assessing and addressing cybersecurity needs of nonprofits.
- The [Federal Trade Commission](#) provides information and links to additional resources for small business (including nonprofits) related to cybersecurity.
- The [Cybersecurity & Infrastructure Security Agency \(CISA\)](#) provides information, tips, and resources for the [Faith-Based Community](#), [High Risk Communities](#) and [Educational Institutions](#).
- CISA also has a more generalized [cyber resource hub](#).

GENERAL RESOURCES FOR NONPROFIT CONTRACTING

New York State has launched the [New York State Nonprofit Unit website](#) as a resource for nonprofits, offering assistance and information to nonprofit organizations seeking to contract with New York State-. Please refer to this page for helpful resources.

Appendix: HATE CRIME INCIDENTS AND POINT ALLOCATIONS

-County	2021	2022	2023	3 YR Total	County Score
Albany	23	36	30	89	5
Allegany	1	0	0	1	1
Bronx	51	41	22	114	5
Broome	3	8	3	14	4
Cattaraugus	2	8	6	16	4
Cayuga	10	6	5	21	4
Chautauqua	3	1	5	9	3
Chemung	1	1	1	3	2
Chenango	1	0	1	2	2
Clinton	5	1	1	7	3
Columbia	1	0	0	1	1
Cortland	0	1	5	6	3
Delaware	2	1	0	3	2
Dutchess	12	8	14	34	4
Erie	15	18	23	56	5
Essex	1	1	0	2	2
Franklin	0	4	1	5	3
Fulton	0	2	2	4	2
Genesee	1	2	0	3	2
Greene	3	1	0	4	2
Hamilton	0	2	0	2	2
Herkimer	0	0	2	2	2
Jefferson	2	1	2	5	3
Kings	131	204	205	540	5
Lewis	0	0	0	0	1
Livingston	0	0	1	1	1
Madison	3	0	5	8	3
Monroe	14	16	7	37	5
Montgomery	0	1	1	2	2
Nassau	32	61	80	173	5
New York	211	238	251	700	5
Niagara	3	4	3	10	4
Oneida	6	8	4	18	4
Onondaga	3	3	4	10	4
Ontario	1	2	6	9	3
Orange	5	8	13	26	4
Orleans	0	0	0	0	1
Oswego	2	4	0	6	3
Otsego	1	1	1	3	2
Putnam	0	0	3	3	2
Queens	106	87	129	322	5
Rensselaer	4	2	0	6	3
Richmond	15	24	22	61	5
Rockland	8	16	27	51	5
Saratoga	2	4	5	11	4
Schenectady	3	9	8	20	4
Schoharie	1	2	0	3	2
Schuyler	0	0	0	0	1
Seneca	1	1	1	3	2
St. Lawrence	6	5	4	15	4
Steuben	1	0	3	4	2
Suffolk	28	28	30	86	5
Sullivan	0	2	1	3	2
Tioga	1	0	0	1	1
Tompkins	2	2	11	15	4
Ulster	5	5	9	19	4
Warren	1	0	0	1	1
Washington	2	0	3	5	3
Wayne	1	0	3	4	2
Westchester	26	40	52	118	5
Wyoming	1	1	0	2	2
Yates	0	1	2	3	2

Source: DCJS, Uniform Crime Reporting system (as of 4/14/2025).

Appendix: *STANDARDIZED PROJECT WORK PLANS*

STANDARDIZED PROJECT WORK PLAN FOR PHYSICAL SECURITY PROJECTS

Goal:

To complete projects to improve the safety and security of the [*XXXXXX* enter name of organization and facility] due to the risk of hate crimes or attacks because of the organization's ideology, beliefs, or mission.

Objective 1:

Reflective of the award, the *XXXXX* organization will identify, purchase, and install the type(s) of indoor and/or outdoor facility hardening measures needed to improve the safety and security of the facility.

Task #1:

The grantee will identify the specific equipment to be purchased and the cost of installation. Establish reasonableness off cost and that the costs are within the contract budget.

Performance Measure:

1. Provide description of equipment to be acquired including cost per unit.
2. Provide description of cost of installation of equipment.
3. Provide a "before" photo(s) showing the project area(s) prior to the completion of any work or installation of equipment.

Task #2:

According to procurement guidelines the grantee will order and install the identified and approved equipment.

Performance Measure:

1. Provide description of equipment and number of units ordered.
2. Provide a narrative describing the process in which the equipment was procured. Include a justification for reasonableness of cost.
3. Provide the date(s) equipment was ordered
4. Provide the date(s) the equipment was installed.
5. Provide a narrative description of the usage and maintenance of any equipment acquired through the grant.
6. Provide photo(s) showing the project area(s) after completion of work or installation of equipment. Photo(s) should be of the completed project in the identified location, from the same perspective as the photos provided in the application and in a manner that clearly demonstrates the work performed.

Objective 2:

To provide necessary training to the organization's/facility's staff and other appropriate individuals to prevent and protect against hate crimes and acts of bias. Training should be limited to topics that improve physical security and/or enhance staff and/or facility users' knowledge of hate crime activity and use of the equipment, suspicious behavior, emergency evacuation procedures, or similar topics that improve the security of the facility and safety of its users.

Task #1:

Identify and procure training to be provided using appropriate procurement requirements.

Performance Measure:

1. Provide a narrative describing the process in which the training was procured. Include a justification for reasonableness of cost.
2. List and describe the type(s) of training provided during the quarter and the name of the organization providing training. If the training was conducted off-site, provide the date and location where the training was held.
3. Identify the number and titles of staff that attended each training(s) during the quarter.
4. Provide date and number of attendees at each training, for example, X number of school students or campers, or X number of worshippers, etc. attended active shooter training

Objective 3:

To implement the provisions of NYS Exec. Law Article 15-A and 5NYCRR Parts 142-144 Minority and Women-Owned Business

Task #1:

Utilize good faith efforts, pursuant to 5 NYCRR 142.8 of the New York State Executive Law Article 15-8, to meet the maximum feasible portion of the organization's established MWBE goals

Performance Measure:

1. What percent of your established Minority and Women Business Enterprise goal have you met to date?

STANDARDIZED PROJECT WORK PLAN FOR CYBERSECURITY PROJECTS

Goal:

To complete projects to improve the cybersecurity of the [XXXXXX enter name of organization and facility] due to the risk of hate crimes or attacks because of the organization's ideology, beliefs, or mission.

Objective 1:

Reflective of the award, the XXXXX organization will identify, purchase, and install software/equipment or conduct planning, training, or testing exercises to improve the organization's cybersecurity.

Task #1:

The grantee will identify the specific equipment or services to be purchased to improve the organization's cybersecurity.

Performance Measure:

1. Provide description of any software/equipment to be acquired including cost per unit and expected number of units/licenses.
2. Provide a narrative describing the process in which the software/equipment was procured. Include a justification for reasonableness of cost.
3. Provide description of cost of installation of any equipment or implementation of software.
4. Provide a description of any planning, training, or testing exercises identified.

Task #2:

According to procurement guidelines the grantee will order and install the identified and approved software/equipment.

Performance Measure:

1. Provide description of software/equipment and number of units ordered
2. Provide a narrative describing the process in which the software/equipment was procured. Include a justification for reasonableness of cost.
3. Provide the date(s) software/equipment was ordered
4. Provide the date(s) the software/equipment was installed.
5. Provide a narrative description of the usage and maintenance of any software/equipment acquired through the grant.
6. Provide photo(s) showing the project area(s) after completion of work or installation of equipment. For software, in lieu of photos, please attach in GMS any and all invoices and receipts.
7. Provide the date(s) and description of any planning, training, or testing services provided during the quarter.

Objective 2:

To implement the provisions of NYS Exec. Law Article 15-A and 5NYCRR Parts 142-144 Minority and Women-Owned Business

Task #1:

Utilize good faith efforts, pursuant to 5 NYCRR 142.8 of the New York State Executive Law Article 15-8,

to meet the maximum feasible portion of the organization's established MWBE goals

Performance Measure:

1. What percent of your established Minority and Women Business Enterprise goal have you met to date?

ATTACHMENTS REQUIRED IN GMS:

Attachment 1 Vulnerability Self-Assessment Tool (PDF download available on our [website](#))

BUDGET DETAIL WORKSHEET AND NARRATIVE GUIDE

ORGANIZATION:

CONTRACT TERM:

Personal Services - Salary - List positions by title. For each position title, show the annual rate of pay, the percentage of time charged against the grant (percent of FTE). **Please enter the percentage as a decimal (ex. 50% should be entered as .50)**

Position	Annual Salary	% FTE of Annual Salary	Cost

Personal Services -Salary Justification: Describe the responsibilities and duties of each position in implementing and operating the grant program.

Personal Services - Fringe - Fringe benefits to be aggregated for the personnel listed above, and only for the percentage of time (%FTE) of each position charged to the project. Fringe should be based on actual known costs or approved negotiated rate of the agency. **Please enter the percentage as a decimal (ex. 50% should be entered as .50)**

Aggregate or Position	Total Salary Paid with Grant Funds	Fringe Rate	Computation (Salary x Fringe Rate)

Personal Services Fringe Justification: Use approved fringe rate for grant related salaries above. Do not break out dollar value of each benefit. An aggregate can be used if all positions have the same fringe rate. If the positions have different fringe rates each position should be lined out separately.

Contractual/Consultant Services - For consultant name, hourly or daily fee, and estimated time on the project. Upload the signed consultant agreement as an Attachment in GMS. Provide type of service in the justification. **If there is an aggregate cost and no hourly or daily rate please enter the total cost in the hourly/daily fee and 1 in the estimated time.**

Consultant Name	Cost of Hourly or Daily Fee	Estimated Time on the Project in Hours	Computation (Fee x Est. time)

BUDGET DETAIL WORKSHEET AND NARRATIVE GUIDE

ORGANIZATION:

CONTRACT TERM:

Contractual/Consultant Services Justification: Explain how the consultant(s) is necessary to the success of the project and discuss the procurement method to be used. Provide explanation of cost to be paid from the grant to the consultant, i.e., fees (limited to \$650 per 8-hour day unless justification is provided and approved by DCJS), travel, meals, and lodging per OSC guidelines unless otherwise approved by DCJS. Any consultant anticipated out-of-state travel must be pre-requested and approved in writing by DCJS.

Travel - Indicate aggregate project related expenses required of staff (for example, for training, field work, meetings). Prior to any out-of-state travel, a written request for approval to use grant funds must be submitted to DCJS for written approval. Also indicate aggregate cost of participant travel if reimbursed, for example, metro cards.

Travel

Cost

Travel and Sustenance Justification: Describe location and purpose of travel, mode of transportation and cost. Also indicate who is traveling and how this travel is necessary for the success of the project. Meals and lodging must not exceed published state per diem rates. Participant cost must be specified, e.g., metro cards

Equipment - List cost of non-expendable program equipment to be purchased and aggregate cost of office equipment to support the grant. (List expendable equipment under the "Supplies" category.) Rented or leased equipment should be included in this category.

Item

Approx. Quantity

Approx. cost per item

Total Cost

Equipment Justification: List included equipment and explain how the equipment is necessary for the success of the project. Describe the procurement method to be used.

Space/Property&Utilities/Rent - Not-for-Profit applicants: Provide cost of rent specifically for the project. Property taxes are not an allowable expense.

Expense

Cost

Space/Property & Utilities/Rent Justification: Describe the cost allocation method for determining how much rent is being charged to the grant.

BUDGET DETAIL WORKSHEET AND NARRATIVE GUIDE

ORGANIZATION:

CONTRACT TERM:

Alterations- Indicate aggregate project related expenses required for alterations.

Alterations	Cost

Alterations Justifications: Provide a brief description of alterations and how it will assist in the mission of the program.

Operating Expense/Supplies- List aggregate cost of program supplies and aggregate cost of office supplies. (Do not line out costs.)

Item	Total Cost
Office/ProgramSupplies	
Operating Expenses	

Operating Expenses/Supplies Justification: Identify the operating expenses and cost (i.e. insurance/bonding, photocopying, advertising etc.) and

All Other/Other Expenses - Identify any expense not eligible for another category.

Expense	Cost

All Other/Other Expenses Justification: Provide total cost for budget period. List each expense and explain how the expense is necessary for the

Budget Summary	
Budget Category	Total Cost
Personal Service -Salary	
Personal Service - Fringe	
Contractual/Consultant	
Travel	
Equipment	
Space/Property/Rent/Own/Utilities	
Alterations	
Operating Expenses/Supplies	
All Other/Other Expenses	
TOTAL OPERATING BUDGET	