NONPROFIT SECURITY GRANT PROGRAM 2019

Focusing on the Investment Justification

http://www.jcrcny.org/securitygrants

David M. Pollock
Jewish Community Relations Council of NY
pollockd@jcrcny.org
Disclaimer

The information herein reflects the best efforts by the JCRC-NY staff to provide answers to common questions regarding the FY2019 DHS Nonprofit Security Grant Program. Grant applicants are urged to revisit the JCRC-NY website (www.jcrcny.org/securitygrants) often since it is updated regularly as new information becomes available.

Applicants should carefully review all of the grant information posted by NY DHSES (or their local SAA if they are outside NY) and consult their own legal counsel or other advisers during the preparation of their application. The following is being provided for educational and informational purposes only, without representation, guarantee or warranty of any kind. The JCRC-NY is not responsible for any injury, loss or damages to persons or property arising from the use or misuse of this information.
NONPROFIT SECURITY GRANT PROGRAM 2019

Part One | The Basics
Who is eligible for grants of up to $100,000?

Two programs
Only at-risk 501(c)(3) nonprofit agencies may apply.

<table>
<thead>
<tr>
<th>NSGP-UASI</th>
<th>NSGP-S</th>
</tr>
</thead>
<tbody>
<tr>
<td>For organizations located</td>
<td>Organizations outside the</td>
</tr>
<tr>
<td>within <strong>31 designated regions</strong></td>
<td>designated regions. Last year,</td>
</tr>
<tr>
<td>In New York State that</td>
<td>5 NY organizations received</td>
</tr>
<tr>
<td>includes: <strong>New York City,</strong></td>
<td>NSGP-S grants.</td>
</tr>
<tr>
<td><strong>Nassau, Suffolk and</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Westchester Counties</strong>. Last</td>
<td></td>
</tr>
<tr>
<td>year, 113 NY organizations</td>
<td></td>
</tr>
<tr>
<td>received NSGP-UASI grants.</td>
<td></td>
</tr>
</tbody>
</table>

All New York applicants must be prequalified, see [https://grantsreform.ny.gov/grantees](https://grantsreform.ny.gov/grantees) and submit their “paperwork” via the E-Grants system, and include all of the necessary documents.
Outside of New York

- Nonprofits located in these 31 UASI-designated areas are eligible for grants up to $100,000 from a total allocation of $50 million for the NSGP-UASI program.
- Nonprofits located outside these areas are eligible for up to $100,000 from a total allocation of $10 million for the NSGP-S program.

<table>
<thead>
<tr>
<th>FY 2019 NSGP Eligible Urban Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Arizona</strong></td>
</tr>
<tr>
<td>Phoenix Area</td>
</tr>
<tr>
<td><strong>District of Columbia</strong></td>
</tr>
<tr>
<td>National Capital Region</td>
</tr>
<tr>
<td>Oregon</td>
</tr>
</tbody>
</table>
1. All not-for-profit organizations must be prequalified in order to do business with New York State and to apply for grants. In order to prequalify, not-for-profit organizations must submit an online Prequalification Application through the Grants Gateway. The Prequalification Application is comprised of five components to gauge your organizational structure and the types of services you provide. The required forms and document uploads are all part of the Document Vault. Click to https://grantsmanagement.ny.gov/register-your-organization to start the process and follow the instructions there.

2. Once your organization is registered you will be provided with a Username and Password allowing you to access the Grants Gateway system. See the Prequalification Documents and Questions for a list of questions included in the prequalification process and explanations of documents that must be included in a prequalification application.

3. Remember: three of a nonprofit’s essential financial documents - the IRS990, Financial Statement and Charities Bureau filing - expire on an annual basis. A nonprofit must upload current versions of these documents for review and approval each year to maintain prequalification.

Confused?? Cyber-phobic?? You need 2 apps

• In order to submit your grant you will need to:
  
  **Prequalify** using *Grants Gateway* and upload documents into a *Document Vault*. Once you are prequalified you should print out the *Status Report* to submit with your application package. [Here’s how.](#)

  **Submit** your application and the required attachments online, via *E-Grants*. There is a great tutorial available to help you navigate the process. When you are ready to submit, simply open up the tutorial in one window and E-Grants in another. [Then fill in E-Grants as the tutorial directs you.](#)

Each system (Grants Gateway and E-Grants) requires registration, a unique account name and a password.
Timing

- NY application packages must be uploaded via the E-Grants system by 5 PM, **May 8, 2019**. The deadline will be strictly enforced. No excuses.

- All of the official forms and requirements will be available at [http://www.dhses.ny.gov/grants/nonprofit.cfm](http://www.dhses.ny.gov/grants/nonprofit.cfm). The information on the NY State website is definitive.

- Successful grantees will have to complete additional paperwork. Even if you do everything expeditiously and correctly, do not expect to be able to access the funding until after January, 2020.

- **Applicants in other states should consult with their own authorities.** Click to the [State Administrative Agency (SAA) Contact List](http://www.jcrcny.org/securitygrants) to find the right contact for your state.
What can you buy with the grant?

All equipment and training should address a specific threat and/or vulnerability, as identified in the nonprofit’s *Investment Justification*. Equipment is for specific “target-hardening” activities:

- **Physical security enhancements.** (e.g. alarm systems, CCTV systems, blast mitigation/security film for doors or windows) AEL Category 14;
- **Inspection and screening systems.** (e.g. walk-through magnetometers and conveyor-belt x-ray systems used to screen personnel and packages for hazardous materials/devices) AEL Category 15; or
- **Security-related planning and training.** physical and cyber security, target hardening, and terrorism awareness/employee preparedness including programs such as Community Emergency Response Team (CERT) training, Active Shooter training, and emergency first aid training. Training conducted using NSGP funds must address a specific threat and/or vulnerability, as identified in the nonprofit’s Investment Justification. Training should provide the opportunity to demonstrate and validate skills learned, as well as to identify any gaps in these skills.

The grant cannot be used for overhead or equipment other than that on the list. It can be used for installation. *Note: you must list the AEL category of selected equipment on the Investment Justification.*

NONPROFIT SECURITY GRANT PROGRAM 2019

Part Two | The Investment Justification
Learn how to read and follow directions

• Rule 1 If you don’t follow directions:
  • You will lose points; or
  • Your application not be considered.

• Rule 2 There is no Rule 2 See Rule 1
Technical tip (Excel worksheet)

When opening the Investment Justification (IJ) template, some users may see a note that says "Security Warning: some active content has been disabled."

1. Click on the [Options …] button next to the message,
2. select "Enable this content," then click on the [OK] button.

If this is not done, the text boxes may not function properly.

The answer boxes will limit the numbers of characters that you can use. If you choose to paste your answers into the spreadsheet, make sure that all the words are actually there.

Go to IJ tab
Putting the pieces together for a good score

**SCORING THE INVESTMENT JUSTIFICATION**

- Developing a plan that identifies and addresses your risks: 70%
- Risk = Threat + Vulnerability + Consequences
- Target Hardening =
  - How well does it mitigate the risks?
  - Does it focus on prevention/protection of terrorist threats?
  - Are the projects allowable?
  - Are the projects feasible?
- Knowing how to implement your plan: 30%

- Background (2) 5%
- Target Hardening (14) 35%
- Risk (12) 30%
- Impact (5) 13%
- Project Management (3) 7%
- Milestones (4) 10%
IJ Section I: Applicant Information

- Legal Name of the Organization
- Physical Address of the Facility to include the City and/or County Name
- Year the Original Facility was Constructed (In NYC: www.nyc.gov/maps)
- Organization Type (400 character max description of organization’s ideology, beliefs and mission – see next slide)
- 501(c)(3) Number (Use your EIN)
- Dun and Bradstreet Number / DUNS (Applications without a DUNS number will not be accepted. To apply for one click here.)
- FY 2019 Urban Area (New York City)
- FY 2019 NSGP Federal Funding Request (no more than $100,000)
- FY 2019 NSGP Total Project Cost
- Any Current Contract with DHS (This does not include any DHS or NSGP grant funds previously awarded to the nonprofit organization.)
- Investment Phase – New (This section will not be scored, but can get you disqualified)
Mission statement

- Each organization must include its Mission Statement and any mission-implementing policies or practices that may elevate the organization’s risk. Recognizing the impact an organization’s ideology, beliefs, or mission may have on their risk of potential terrorist threats, NY DHSES will use your Mission Statement, along with information provided in your application to validate the organization type. The central purpose of the organization described in the Mission Statement will be used to validate the organization as one of the following:
  1. Ideology-based/Spiritual/Religious (scores multiplied by a factor of three);
  2. Educational or Medical (scores multiplied by a factor of two);
  3. Other (scores multiplied by a factor of one).

- Terrorism experts think that houses of worship and other facilities associated with religious groups will continue to be targets of interest for foreign terrorist organizations and their followers in the West.
  - If you are a religious corporation, make it explicit, e.g., start with: “We are a NYS religious corporation...” If you are religiously-affiliated, say so.
II Section II: Background Information

- **Background:** Describe the nonprofit organization including:
  - Membership and community served
    - services offered; and
    - populations served
    - Let the judges know about the number of people served by your various offerings.
  - Symbolic value of the site(s) as a highly recognized national or historical institution that renders the site as a possible target of terrorism
  - Any role in responding to or recovering from terrorist attacks (e.g., pastoral care for community)
  - Your answer should set the context for, and relate to, the other questions.

(Worth up to 2 of 40 points.)
Develop effective answers with these steps:

1. **Determine the most likely terrorism-related threats** (thoroughly addresses findings from previously conducted risk assessments, police reports, and/or insurance claims).
2. **Survey your facility** to identify and describe your physical security vulnerabilities (i.e., the organization's susceptibility to destruction, incapacitation, or exploitation by a terrorist attack?).
3. **Prioritize your vulnerabilities** by focusing on high consequence/high probability events.
4. **Pinpoint the target-hardening steps** needed to mitigate the identified risk(s) and/or vulnerabilities by **deter**ring an attack, **deny**ing an attacker access, **delay**ing an attack or **mitigate** the damage of an attack. All of the target-hardening steps must be allowable (i.e., listed on the **Authorized Equipment List**) and feasible.
## Parsing the risk section (30% of your score)

\[ \text{risk} = \text{threat} + \text{vulnerability} + \text{consequences} \]

<table>
<thead>
<tr>
<th></th>
<th>IJ Question</th>
<th>How you will be scored</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat</strong> (4 points)</td>
<td>In considering threat, the applicant should discuss the identification and substantiation of specific threats or attacks against the nonprofit organization or closely related organization by a terrorist organization, network, or cell. The applicant should also discuss findings from a risk assessment, police findings, and/or insurance claims specific to the location being applied for including dates and specific threats.</td>
<td>How well did the applicant address findings from previously conducted risk assessments, police reports, and/or insurance claims?</td>
</tr>
<tr>
<td><strong>Vulnerability</strong> (4 points)</td>
<td>In considering vulnerabilities, the applicant should discuss the organization's susceptibility to destruction, incapacitation, or exploitation by a terrorist attack.&quot;</td>
<td>How well did the applicant address the organization's susceptibility to destruction, incapacitation, or exploitation by a terrorist attack?</td>
</tr>
<tr>
<td><strong>Consequences</strong> (4 points)</td>
<td>In considering potential consequences, the applicant should discuss potential negative effects on the organization's asset, system, and/or network if damaged, destroyed, or disrupted by a terrorist attack.</td>
<td>How well did the applicant address potential negative effects on the organization's asset, system, and/or network if damaged, destroyed, or disrupted by a terrorist attack?</td>
</tr>
</tbody>
</table>
See the JCRC’s “Selected Threat Scan” for specifics and [http://www.jcrcny.org/security-justification5/](http://www.jcrcny.org/security-justification5/)

<table>
<thead>
<tr>
<th>What happened to you?</th>
<th>Identify terrorist-related threats and hazards</th>
<th>Assess risk</th>
<th>Prioritize threats and hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include information from previously conducted risk assessments, police reports, and/or insurance claims.</td>
<td>Based on events at similar or nearby facilities: e.g., active shooters or using sharp-edged weapons, explosive devices, arson, mail and package attacks</td>
<td>Which are the terrorist-related threats and hazards that are most likely to occur and which will cause the most serious consequences?</td>
<td>Address the vulnerabilities related to high-risk/high consequence threats first.</td>
</tr>
</tbody>
</table>
Terrorist Attack Tactics

- **What:** The most likely tactics in a hypothetical terrorist attack here in the U.S. would likely involve simple tactics such as vehicular assaults, edged weapons, small arms, arson, and possibly improvised explosive or incendiary devices (IEDs/IIDs).

- **Possible targets:** Often, violent extremist and terrorist organization messaging often focuses on densely populated areas, police and military and large gatherings. Some groups provide detailed tactics and techniques to exploit perceived vulnerabilities.

Highlight the gaps found in your “previously conducted risk assessment” (you must submit the vulnerability/risk assessment on which the request in the Investment Justification is based).

- Lack of, or weak physical protective measures
- Lack of adequate access control and insufficient screening of individuals
- Lack of hardware to support sound security policies
- Facility does not have an active shooter plan and the employees not trained in active shooter procedures

Prioritize by identifying high-probability/high consequence threats.

Help with the identification of vulnerabilities
- NJ: Facility Self-assessment Tool
- CA: Protective Measures for Enhanced Facility Security
### Tying together the risk and target hardening language

<table>
<thead>
<tr>
<th>14EX-00-BSI (Systems, Building, Blast/Shock/Impact Resistant)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems to mitigate damage from blasts, shocks, or impacts, such as column and surface wraps, wall coverings, breakage/shatter resistant glass, window wraps, and deflection shields.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sample vulnerability language</th>
<th>Sample target hardening language</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are large glass windows around the lobby and windows in virtually every ground floor and second floor space (offices, meeting rooms and classrooms). These windows, especially those in the back of the building, would provide a hostile intruder ready access to the building. The blast effect of an improvised explosive device (IED) placed outside of the building -- near the building --could cause extensive physical damage to the building and turn these windows into razor-like shards, resulting in multiple injuries.</td>
<td>At minimum, it is recommended that all windows, doors, and other glass features within eighteen (18) feet of the ground or with direct exposure to neighboring buildings should be equipped with locks and properly anchored forced entry resistant security/blast mitigation film or that the existing glass be replaced with security laminated glass that meets forced entry resistance standards. The blast mitigation film could deter, delay and deny entry to the building while mitigating the injuries from a blast.</td>
</tr>
</tbody>
</table>
Hiring of contracted security personnel is now allowed under this program (see the FEMA update here).

- NSGP funds may not be used to purchase equipment for contracted security guards. These costs should be classified as organization costs.
- Subrecipients (grantees) may not use NSGP funding to hire full or part-time employees that are currently, or will be placed on a nonprofit’s payroll.
- Rob Goldberg of JFNA reports after speaking with FEMA, that the blanket waiver WILL be in place and interested organizations may now request up to 100% of their total award towards the cost of contacted security personnel.

**JCRC comment:** Make a case for security guards through an identified vulnerability included in your assessment (e.g., failure to review or monitor CCTV recordings for possible instances of hostile surveillance, inadequate access control measures and an inability to interdict a hostile intruder, and or the lack of security guards during all hours of operation) and add “Contracted security guards” as an “Item to be purchased” in IV. Target Hardening (Note: there is no AEL number for Contracted security guards).

Recipients of NSGP funding may use the grant to pay for contracted security personnel over the entire three year period of the grant. However, grantees should not assume that they will be successful applicants in coming years (you might not win a grant or this program may not exist in coming years) so you should be able to sustain this capability in future years without NSGP funding.

- A case can readily be made for additional contracted security guards, additional hours or an upgrading replacement (e.g., unarmed to armed) of the existing guards.
- Finally, we think that it is appropriate to remind you that security guards are no panacea. Security planning should entail a well-considered mix of personnel, plans, procedures, training, drills and exercises and security hardware. The judges tend to look at your assessments to see if you are addressing the most important vulnerabilities.
Tying together the risk and target hardening language

**Contracted Security Guards (no AEL number)**

*Hiring of contracted security personnel is allowed under this program.*

<table>
<thead>
<tr>
<th>Sample vulnerability language</th>
<th>Sample target hardening language</th>
</tr>
</thead>
<tbody>
<tr>
<td>• There are inadequate access control measures at the main entrance, including the absence of security personnel, leading to an inability to interdict a hostile intruder.</td>
<td>Retain contracted security guards and deploy them in a visible manner, whenever the facility is open. Develop post orders that include the implementation of the access control procedures as specified by the facility and a daily review of the CCTV recordings.</td>
</tr>
<tr>
<td>• CCTV systems are not monitored or reviewed for possible instances of hostile surveillance</td>
<td>Contracted security guards can deter hostile intruders, deny them, or at least delay their entry to the facility. Guards can also trigger both audible and central station alarms which could mitigate damage and injury.</td>
</tr>
<tr>
<td>• Security personnel are only deployed during Sabbath and holiday services.</td>
<td></td>
</tr>
</tbody>
</table>
III.C. Potential Consequences

- **Human toll.** The only consequence more dire than the loss of life is a multi-casualty event. Both are possible as the result of a terrorist attack. Injuries -- ranging from minor to life threatening -- are probable. Incapacitation is a very real consequence.

- **Physical plant.** In the event of an improvised incendiary device (IED) left on the scene or contained by a vehicle, your building housing could be badly damaged or completely destroyed.

- **Reputational damage**
  - **Physical attack.** The parents and student body are quite confident that the school is a safe and secure environment. An attack would shatter that opinion, making it difficult for the school to reestablish itself after an attack.
  - **Cyberattack.** Visitors to organizational websites and people who provide identifying data (e.g., SSN’s, DOB, Bank routing information, credit cards) implicitly trust the organizations with which they interact. That trust can be destroyed by a breach.

- **Secondary outcomes.** For example if members of the faculty hold positions in other institutions, those other institutions would be adversely affected by their death or incapacitation. Similarly, the employment status of the parents of students might be jeopardized if your organization could not care for their children during working hours.

Question: In considering potential consequences, the applicant should discuss potential negative effects on the organization’s asset, system, and/or network if damaged, destroyed, or disrupted by a terrorist attack.
• Provide a thorough description of how each of the proposed target hardening activity will mitigate the identified risks listed in your risk assessment
  • (e.g., in conjunction with sound access control policies and procedures, new doors will deter a terrorist attack, delay an intruder and mitigate damage because it would give law enforcement the time to respond and address the threat before an attacker can accomplish his/her goal.)

• Make sure that your hardware program thoroughly focuses on the prevention of and/or protection against the risk of a terrorist attack?
Don’t make the reviewers go searching

- Use this chart to your advantage. Make “Item to be Purchased” #1 clearly tied to “Vulnerability to be Addressed” in the previous section. Label it #1.

- **NEW** NSGP: Tying together the risk and target hardening language

(2,200 character limit, worth 14 of 40 points)
Planning

Funding may be used for security or emergency planning expenses and the materials required to conduct planning activities. Planning must be related to the protection of the facility and the people within the facility and should include consideration of access and functional needs considerations as well as those with limited English proficiency. Examples of planning activities allowable under this program include:

- Development and enhancement of security plans and protocols.
- Development or further strengthening of security assessments.
- Emergency contingency plans.
- Evacuation/Shelter-in-place plans.
- Other project planning activities with prior approval from DHS/FEMA.
IV. Target Hardening: Training

• Nonprofits are *encouraged* to apply for additional costs including security training for all nonprofit staff, planning related costs, and exercises related cost, in addition to allowable equipment.

• Allowable training topics are limited to the protection of critical infrastructure and key resources, including physical and cyber security target hardening, and terrorism awareness/employee preparedness.

• Exercises are allowable because they afford organizations the opportunity to validate plans and procedures, evaluate capabilities, and assess progress toward meeting capability targets in a controlled, low-risk setting.

• Training conducted using NSGP funds must address a specific threat and/or vulnerability, as identified in the nonprofit organization’s investment justification (IJ). Proposed attendance at training courses and all associated costs must be included in the nonprofit organization’s Investment Justification.

• *All training requires DHSES pre-approval.*
The best plans include equipment, planning and training

- Your security equipment should support your security policies.
- Tens of thousands of dollars can be spent on equipment, but the money will be wasted unless you develop robust plans, policies and protocols and your staff is properly training to implement them, with the assistance of security hardware. For example:
  - Cameras are good for investigative purposes, but rarely protect unless trained personnel are viewing the monitors to detect suspicious activity.
  - Access control measures are only effective in support of sound access control policies and protocols.
NONPROFIT SECURITY GRANT PROGRAM 2019

Part Four: Administration (Milestones, Project Management, Impact & Scoring)
V. Milestones

• Provide description and associated key activities that lead to the milestone event over the FY 2018 NSGP period of performance. Start dates should reflect the start of the associated key activities and end dates should reflect when the milestone event will occur.

• Provide specific milestones that present a clear sequence of events that leads to the completion of your project.

• Present a clear sequence of events that effectively build upon each other.

• Describe the milestones as well as associated key activities. For example, “receiving the grant” is a milestone, as is completing the initial state paperwork. An associated key activity is EHP approval.

• Your first Milestone is, “Include Milestones that are specific to your organization (e.g., progress report to the Board)

• Make sure that your Milestones cover state requirements.

• Don’t leave any of the blanks unfilled. Limit yourself to 10 milestones. Each can have one, or more associated key activities.

(4 of 40 points)
### Milestones

1. **Grant award contract.** Associated events: Notice of award, EHP review, completion of other contract requirements, approval of nonprofit board, receipt of signed contract.

2. **Awarding bids for projects 1-3 and door.** AE’s: signed contract with DHSES, rec bids in accordance with NYS procurement rules, eval of bids by board, notifying vendors.

3. Installation of projects 1-2 AE’s: Selection of vendor, scheduling of work, installation, approval of work, payments to vendor.

4. Installation of project 3 AE’s: Selection of vendor, completion of project 1, scheduling of work, installation, payments to vendor.

5. Required reports to NY DHSES. AE’s: quarterly progress reports, reimbursement requests.

6. Installation of doors. AE’s: Selection of vendor, application to landmarks board, approval of landmarks officials, scheduling of work, installation, approval of work, payments to vendor.

7. Progress reports to board and committees.

---

Don’t just copy these steps, the judges want to see specifics related to your projects.
Use this question to describe the staff and board members who will manage the investment of up to $150,000. You should thoroughly justify the effectiveness of the proposed management team's roles and responsibilities and governance structure to support the implementation of the Investment?

You might include the experience of the individual, especially in the management of construction-related projects and the management of a large budget. Your answer should also reflect the professional background of various board members, e.g., real estate, accounting, security, law.

Finally, you should note that your board of directors or a committee will review the proposals, the bids and receive progress reports on the project.

(Worth 3 of 40 points)
VII. Impact

What measurable outputs and outcomes will indicate that this investment is successful at the end of the period of performance?
(2,200 character max - not including spaces)

**Supporting the NPP**

These investments will:
- improve the ability of our organization to prevent a threatened, or an actual act of terrorism, and to protect our constituencies and assets against the greatest threats and hazards;
- strengthen governance integration between private nonprofit entities and Federal, state, and local governments; and
- encourage a whole community approach to security and emergency management.

Which specific National Preparedness Goal (the Goal) core capabilities does this investment work to achieve? Explain how this Investment supports the building or sustaining of these Goal core capabilities. For more information on the Goal see: http://www.fema.gov/national-preparedness-goal.
Your project should further the National Preparedness Goals (https://www.fema.gov/national-preparedness-goal) in one or more of the following categories:

- **Preventing** a threatened or an actual act of terrorism;
- **Protecting** our citizens, residents, visitors, and assets against the greatest threats and hazards;
- **Mitigating** the loss of life and property by lessening the impact of future disasters;
- **Responding quickly to save lives**, protect property and the environment, and meet basic human needs in the aftermath of a catastrophic incident; and/or
- **Recovering** through a focus on the timely restoration, strengthening, and revitalization of infrastructure, housing, and a sustainable economy, as well as the health, social, cultural, historic, and environmental fabric of communities affected by a catastrophic incident.

The FY 2018 NSGP objectives are to support efforts that:

- Build and sustain core capabilities;
- Strengthen governance integration between private nonprofit entities and Federal, state, and local governments; and
- Encourage a whole community approach to security and emergency management.
Sample outcomes

Upon completion, all of the components in our project will be installed and operational and protect our people and assets against terrorist threats.

• **Access Control and Identity Verification.** The proposed access control systems will provide for capacity to screen and authorize all building users and visitors, limiting access to only authorized individuals to carry out legitimate activities.

• **Physical protective measures.** The proposed upgrades to our doors to forced entry standard, together with revised access control procedures will reduce 60% of the identified vulnerabilities by controlling entry to and movement within our building.

• **Blast mitigation film.** The installation of blast mitigation/security film on the ground level windows (50% of the total) will reduce injury, the loss of life and the destruction of property by lessening the impact of an IED.
Funding history/Scoring

- Preference will be given to nonprofit organizations that have not received prior years funding. Applicants that have not received NSGP funding in the past will receive an additional ten (10) bonus point to their total *state application score* at the time of submission to FEMA.

- To calculate an application’s final score, the sum of the applicant’s state score and the average of the two Federal reviewers’ scores will be multiplied by a factor of three (3) for nonprofit groups that are at a high risk of terrorist attacks due to their ideology, beliefs or mission, by a factor of two (2) for medical and educational institutions, and by a factor of one (1) for all others.

- A perfect score for nonprofit groups that are at a high risk of terrorist attacks due to their ideology, beliefs or mission is 240 (State score 40, Federal score average 40 times three). Groups that never received a grant can score 250.
Grade your own work!

The judges, at the state and federal levels, score each question on your Investment Justification using defined criteria. They look at each section and determine if your answer was:

- blank;
- incomplete because it did not include all of the required information;
- complete, but only minimally provided the required information;
- complete, but only moderately provided the required information; or
- complete, and fully provided the required information.

[Image of a scoring worksheet]

YourNY E-Grants checklist

Questions within the E-Grants app

- Contact Information
- Proposed Project Workplan Information
- Budget Request Information
- Certification to Accept the Assurances

E-Grants Attachments

- Investment Justification
- Status History report from Grants Gateway website showing prequalification status
- Signed and notarized Vendor Responsibility Questionnaire or a copy of your on-line Questionnaire certified within the last six months
- Mission Statement
- Threat and/or vulnerability assessment for each facility listed on each Investment Justification

Note: The E-Grants system will not allow you to submit unless you have completed the appropriate steps. See the FY 2019 NSGP E-Grants Tutorial.
If you’re not in NY, get the details right

• Know your state’s application submission deadline. And don’t wait until the last minute.
• If you don’t pay attention to the directions, your application won’t be considered.
For more information:

- [http://www.dhses.ny.gov/grants/nonprofit.cfm](http://www.dhses.ny.gov/grants/nonprofit.cfm)
- [http://www.jcrcny.org/securitygrants](http://www.jcrcny.org/securitygrants)

- David Pollock
  
  Associate Executive Director and Director, Public Policy and Jewish Security, JCRC-NY
  
  (212) 983-4800 x132/*pollockd@jcrcny.org*

- DHSES Application Information
  
  NYS Division of Homeland Security and Emergency Services Contracts Unit
  
  1220 Washington Ave., Bldg. 7A Suite 610
  
  Albany, NY 12242 (866)-837-9133
  
  Email: grants@dhses.ny.gov

- Grants Gateway Help
  
  grantsgatewayhelp@its.ny.gov (518) 474-5595
  
  Valerie Bloomer valerie.bloomer@dhses.ny.gov