The Jewish Federations® of North America
Washington Office

THE STRENGTH OF A PEOPLE.
THE POWER OF COMMUNITY.

Preliminary Guidance

The Department of Homeland Security (DHS) Nonprofit Security Grant Program Funding Opportunity FY2021

JFNA Grant Application Guidance

October 23, 2020

Point of Contact: Rob Goldberg, Senior Director, Legislative Affairs, at:
rob.goldberg@jewishfederations.org

[The following is preliminary guidance based on the most recent DHS Notice of Funding Opportunity (for FY 2020). Once the FY 2021 NOFO is published, we will provide supplemental guidance reflecting any new information, modifications or changes.]

[Note: For all New York-based communities/organizations, see footnote below[1]]

For the purposes of this grant:

- Nonprofit organizations are **sub-applicants**;
- State Administrative Agencies (SAAs), typically the state homeland security & emergency management agency, administer the program locally, score and prioritize sub-applications, and submit the applications for federal review on behalf of the sub-applicant nonprofit organizations;
- The Federal Emergency Management Agency (FEMA) administers the program nationally, reviews and further assesses (based on national threat considerations) the submissions and makes funding recommendations to the Secretary of Homeland Security ; and
- The Secretary of Homeland Security makes the final award determinations.

Note: Nonprofit sub-applicants work only through their State Administrative Agencies and not directly with FEMA.

---

[1] Before Proceeding, all New York base communities/orgs, should contact David Pollock, Associate Executive Director, and Director of Public Policy & Security, JCRC of New York, on all matters pertaining to the NSGP application process at: pollockd@jcrcny.org / http://www.jcrcny.org/security. New York State has very particular requirements for which David is expert. He and I otherwise collaborate, and he incorporates my guidance into his own, as applicable.]

The following guidance is organized to assist eligible nonprofit organizations (**sub-applicants**) with completing the grant application, which is called an **Investment Justification (IJ)**, a sample copy of which is attached. There are 7 parts to the IJ, and each section below corresponds to a specific part. Most sections of the IJ will be scored with a best possible raw score of **40 points**. Each section is assigned a set value. As explained in the document, a sub-applicant must also submit a **Mission Statement** and **Risk/Vulnerability Assessment** along with the IJ when applying.

Note: The raw score will be weighted by a number of factors that will impact each sub-applicant's ranking. This includes **the "type" of nonprofit that is applying** and whether the nonprofit has previously received an award. This is explained in greater detail below.

Grant Application: Part I. Sub-Applicant Information
(This section is not scored)

The first section of the IJ is the Sub-Applicant Information Section, which requests the following Information:

1. Legal name of organization
2. Physical address of the organization
3. Year the facility was constructed
4. **Organization type***
5. **Membership & community served****
6. Organization's 501(c)(3) number (if applicable)
7. **Current Dun & Bradstreet number*****
8. The applicable Urban Area (NSGP- UA only)[2]
9. **Funding amount requested (up to $100 thousand)******
10. Total project cost
11. Verification of any current DHS contract
12. New or ongoing investment

Notes:

* **Organization Type (i.e., ideology, beliefs and mission):** This question provides the first substantive opportunity for a sub-applicant to: a) address the institution's intrinsic nature that

[2] There were thirty-two designated UASI areas in FY 2020: Phoenix Area (AZ); Anaheim/Santa Ana Area, Bay Area, Los Angeles/Long Beach Area, Riverside Area, Sacramento Area, San Diego Area (CA); Denver Area (CO); National Capital Region (DC, parts of MD and VA); Miami/Fort Lauderdale Area, Orlando Area, Tampa Area (FL); Atlanta Area (GA); Honolulu Area (HI); Chicago Area (IL); New Orleans (LA); Baltimore Area (MD); Boston Area (MA); Detroit Area (MI); Twin Cities Area (MN); St. Louis Area (MO); Las Vegas Area (NV); Jersey City/Newark Area (NJ) New York City Area (NY); Portland Area (OR); Philadelphia Area, Pittsburgh Area (PA); Dallas/Fort Worth/Arlington Area, Houston Area, San Antonio Area (TX); Hampton Roads Area (VA); Seattle Area (WA). These designations may differ slightly from year-to-year. We will update for FY 2021.

may make it a potential target of terrorism. In drafting a response, it is critical to the scoring to clearly state how the sub-applicant is one or more of the following categories:

1. Identifiable as Jewish or faith-based;
2. Ideologically pro-Israel or pro-Jewish; and/or
3. Grounded in Jewish values, learning, heritage or life.

How a sub-applicant describes itself (Organization Type) will have a substantially impact on their final score (See "Final Scoring" on Page 12).

Mission Statement: Similarly, a sub-applicant must include a Mission Statement and any mission implementing policies or practices that may elevate the organization's risk. The Mission Statement along with information provided in the sub-applicant's IJ will be used to validate the organization is one of the following types: **1) Ideology-based/Spiritual/Religious**; 2) Educational; 3) Medical; or 4) Other.

All sub-applicants will want to identify as the first type to maximize their final score.

** **Membership & Community Served:** This question also provides an opportunity to amplify the organization as a likely targeted of a terrorist threat. The following are recommendations to consider:

1. A sub-applicant may participate in a task force, community-relations council, or other **community advisory group** as a representative of the Jewish community. If so, they may want to include this information in the application.

2. An organization, its staff, or volunteers may sponsor, host, participate in, or otherwise be a part of a **local community event** (i.e., a parade, fund raiser, block party) that would place a spotlight on the institution. If so, they may want to include this information in the application.

3. A sub-applicant may be a **center of Jewish communal activity** with a regular monthly schedule of public activities that are widely known and publicized, including on the Internet or through other media. If so, they may want to include this information in the application.

*** **Dun & Bradstreet Number**: This is requisite of all sub-applicants. To register or search for an existing DUNS Number, go to: **http://fedgov.dnb.com/webform/displayHomePage.do**.

****Funding Amount:**

1. Depending on total NSGP FY 2021 appropriations, as established by Congress, the funding cap might increase above last year's $100 thousand cap. This determination will be known once FEMA publishes its FY 2021 grant guidance.

2. This past year, the funding cap was the same between NSGP-UA and NSGP-S. However, under NSGP-S, the state Administrative Agency had discretion to set limits below the cap in order to make more awards. Last year, FEMA allocated states minimum funding levels between $300 thousand and $1.7 million. For some states, the level of funding and level of demand were factors in deciding to lower the cap. Should Congress appropriate increased funding for NSGP-S in FY 2021, state minimum funding allocations set allocations might increase. This determination will be known once FEMA publishes its FY 2021 grant guidance.

System for Award Management (SAM): DHS/FEMA does not require nonprofit organizations to register with SAM.gov. However, **some states do require it**. States that require it will include the requirement in their Notice of Funding Opportunity. It may take four weeks or more for SAM registration to activate. Typically, states will require only funded sub-applicants (post award determinations) to register and the registration must be completed before projects can commence. Information on SAM can be found at: **https://sam.directory/?gclid=EAIaIQobChMIvIyJ9dH05gIVBqSzCh2JAwtlEAAYASAAEgK7mfD_BwE**.

Grant Application: Part II. Background
(This section is worth up to 2 points)

The Background section seeks the following information:

1. **Symbolic value** of the site(s) as a highly recognized national or historical institution or significant institution within the community that renders the site as a possible target of terrorism; and

2. Any **previous or existing role** in responding to or recovering from terrorist attacks.

The following recommendations are intended to assist sub-applicants to think about and formulate their responses.

Symbolic value of the site(s) as a highly recognized national or historical institution that renders the site as a possible target of terrorism:

1. **Recommendation Tailored to Federations and Federation-Affiliated Agencies:** If a sub-applicant is a Federation or a beneficiary/affiliated agency of a Federation, they may want to include the following information in the application:

   "We belong to a widely recognized national/international system with more than 100 years of service to this country: The Jewish Federations of North America. JFNA includes 146 Jewish Federations and over 300 Network communities across North America. Collectively, we are among the top 10 charities on the continent. Our mission is to protect and enhance the well-being of Jews at home and abroad through social welfare,

social services and education. The JFNA system is made up of Jewish Federations, Congregational Schools and higher learning, Jewish Community Centers, Jewish Day Schools, Jewish Family Service Agencies, Jewish Hospitals, Jewish Nursing Homes, and Jewish Vocational Services, among others. Th**e system is the central address of North American Jewry**, employing more than 230,000 people and serving approximately one million clients, annually. The Jewish Federations reach more Jews than any other organization in the world."

2. **Recommendation Tailored to Synagogues and Community Centers**: Synagogues, community centers (and other institutions) may be located **in historic communities, neighborhoods, districts, and/or buildings**. If designated as such by a historical society, local government or municipality, a sub-applicant may want to include this information in the IJ.

Notes:

Even if not officially designated a historic site, many institutions (or their previous iterations) have been operating/located in their communities, neighborhoods, and/or buildings for many decades (some for more than 100 years). If so, a sub-applicant may want to include this information in the application.

If a synagogue, community center (or other institution) is affiliated with a national movement, a sub-applicant may want to include the movement's scope and history in a similar manner as set forth in Recommendation 1, above, when responding to this question.

Synagogues and JCCs are easily identified as centers of Jewish life, and even broader community life and engagement.

3. **Recommendation Focused on Public Recognition:** A sub-applicant may have received an award/awards or other form of public recognition, commemoration, and/or media attention for its work or service from a government agency, association or other professional organization, the press, or other group, singling them out/making them more recognizable. If so, an applicant may want to include this information in the application.

4. **Recommendation Focused on Community Leaders:** A sub-applicant's membership or leadership may include celebrities or community leaders, who are highly recognized national or local figures and whose affiliation with the sub-applicant may raise its profile. If so, they may want to include this information in the application.

5. **Recommendation Focused on Jewish Identity:** If a sub-applicant's name, mission, signage, social media or marketing make it easily recognizable as a Jewish institution or otherwise widely known in the community as a Jewish institution, they may want to include this information in the application.

Any role in responding to or recovering from terrorist attacks:

In responding to this question, a sub-applicant should explain the organization's specific or predominant role(s) played or expertise provided in emergency response/disaster recovery situations, using illustrations where possible. The following information is intended to assist sub-applicants understand and articulate their roles in disaster recovery for purposes of the application. Two critical points that could be made when answering this question:

1. The sub-applicant's **role in emergency response**: to save lives, protect property and the environment, and meet basic human needs in the aftermath of a catastrophic incident; and

2. Its **role in recovery**: 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.

Note: In times of emergency, whether man-made, such as a terror attack, or natural disaster, such as a hurricane or wildfire, consider what role the organization plays on behalf of the community. Examples may be as straightforward as the sub-applicant **sharing vital information with the community (i.e., security alerts; hosting security briefings; organizing security-related community action); raising emergency funds; serving as a central point of contact with government agencies/first responders/other coordinating bodies, such as Federation; providing supports and services to community members/government agencies/first responders/other coordinating bodies.**

For some sub-applicants, this might be a difficult question to answer if they do not have a clear role in emergency response or recovery. In those situations, to make the case that **faith-based and nonprofit organizations provide essential support in disaster relief**, they may want to explain recent event(s) and the role(s), mission, activities they engaged in to mitigate suffering and help victims survive. Possible examples:

1. The organization may **participate in or be affiliated with a local, state, or nationally coordinated effort/network** with government and/or non-governmental partners and/or programs on disaster response (i.e., **VOAD or JVOAD**). If applicable, they may want to identify the entities and discuss the relevant plans, procedures, policies, training, credentialing, and goods and services offered/stockpiled (i.e., food, water, shelter, commodities, equipment, financial assistance, health, social, and/or other humanitarian services (including pastoral services)), and the intended care recipients or beneficiaries.

2. The organization may have **established their own internal or independent program(s)**. If applicable, they may want to identify and discuss relevant plans, procedures, policies, training, credentialing, and goods and services offered/stockpiled (i.e., food, water, shelter, commodities, equipment, financial assistance, health, social, and/or other

humanitarian services (including pastoral services)), and the intended care recipients/beneficiaries.

3. The organization may **contribute to the "Whole Community" approach to homeland security.** The Department of Homeland Security believes it is imperative to integrate and synchronize policies, strategies, and plans -- among all federal, state, local, private, and community efforts across all partners in the professions of prevention, protection, response and recovery – into a unified system for homeland security. They call this a "whole Community" approach to homeland security. If applicable, explain how.

4. If applicable, the organization may want to explain how its institution, agency, or network has successfully **contributed to, coordinated or collaborated and/or partnered with federal, state or local law enforcement or other bodies in emergency response**, disaster recovery, or even more ordinary humanitarian programs or projects serving at-risk populations (i.e., participation on the local board of FEMAs Emergency Food and Shelter Program; coordination with the local Area Agency on Aging to serve homebound senior citizens; providing after school programming for at-risk youths; etc.)

Grant Application: Part III. Risk

(This section is worth up to 12 points)

The Risk section focuses on three questions pertaining to *Threat, Vulnerabilities; and Potential Consequences* of an attack, broken down as follows:

Threat (Part A): The sub-applicant should discuss the identification and substantiation of prior threats or attacks against the organization or a closely related organization by a terrorist organization, network, or cell (to include both foreign and domestic terrorists or violent homegrown extremists). **Proofs should include any findings from a previously conducted vulnerability assessment (see below), police findings, and/or insurance claims specific to the location.**

In answering this question, a sub-applicant should (in order or priority):

1. Describe **specific terror (or violent homegrown extremist) incidents**, threats, hate crimes, and/or related vandalism, trespass, intimidation, or destruction of property that have targeted its property, membership or personnel.

Note: This may also include a specific event or circumstance that impacted an affiliate or member of the organization's system or network.

2. Report on **incidents/threats that have occurred in the community** and/or State where the organization is located.

3. Reference the **public record regarding incidents/threats against similar or like institutions** at home or abroad.

Note: With respect to referencing the public record, I **will provide a Threat Report (shortly)** that aggregates numerous recent threat incidents targeting Jews and Jewish institutions that have been reported in the public record and **will update the report nearer to application time**. Since there is limited working space in the IJ, the sub-applicant should be selective in choosing appropriate examples to incorporate into the response: **events that are most recent, geographically proximate, and closely related to their type or circumstance of their organization or are of such magnitude or breadth that they create a significant existential threat to the Jewish community** at large.

Vulnerabilities (Part B): The sub-applicant should explain the ways the organization is susceptible to destruction, incapacitation, or exploitation by a terrorist attack, threat or intimidation. In answering this question, they should **utilize/rely on the findings from a previously conducted risk/vulnerability assessment in establishing the gaps in security.**

Potential Consequence (Part C): The sub-applicant should discuss potential negative impacts on their assets, system, and/or network if damaged, destroyed, or disrupted by a terrorist attack, threats or intimidation. In answering this question, they **should explain the potential harm that could result from an attack** (i.e., loss of life, disruptions to work or delivery of service, negative economic impact on the sustainability of the organization to remain in business/serve the community).

Note: Each sub-applicant must include a risk/vulnerability assessment on which their application is based, and which is to be submitted with the application to the state agency administering the application process. **The risk/vulnerability assessment is the foundation by which to identify and prioritize resources to address the most critical needs and to ensure transparent, accountable and effective use of grant funds to address identified gaps in existing capabilities**. ← These details are essential to completing this section (Part III) and the following one (Part IV).

Obtaining a risk/vulnerability assessment: Often **local police departments** or **Department of Homeland Security Protective Services Advisors** will conduct such an assessment, as do **private companies**. If your organization is served by a **community security director** or **regional security advisor**, they may be able to conduct the risk/vulnerability assessment. Our colleagues at the **Secure Community Network (SCN)** may be able to help, as described in Recommendation 3, below. There are also **self-assessments** that can be utilized.

Grant Application: Part IV. Target Hardening & Training

(This section is worth up to 14 points)

In this section, a sub-applicant should **explain how the Target Hardening investments will address the *Threat, Vulnerabilities; and Potential Consequences* identified in Part III**.

Note: There MUST be a clear, cohesive and rational flow between the risks identified in Part III and the solutions (or investments) identified in Part IV. Part III serves to explain the risks, vulnerabilities, and consequences of an attack or threat. Part IV describes the recommended improvements from the eligible equipment list (and training/exercises) that would best address and minimize the identified risks, vulnerabilities, and consequences. There should be a flow between these sections; together they establish that the sub-applicant fully understands their vulnerabilities and the best approaches to mitigating the risks.

General Allowable Costs: The sub-applicants may only use the NSGP grant funds for the following permissible uses, and for only those purposes specifically included in the IJ and approved in the award:

1. **Equipment:** Funding is limited to target hardening and physical security enhancements. This includes the acquisition (purchase or possible leasing) and installation of security equipment on real property (including buildings and improvements) owned or leased by the nonprofit organization, specifically in prevention of and/or protection against the risk of a terrorist attack. This equipment is limited to select items within two categories on the **Authorized Equipment List (AEL)**:

   - **Physical Security Enhancement Equipment (Section 14)**
   - **Inspection and Screening Systems (Section 15)**

   The two allowable prevention and protection categories and equipment standards for the NSGP are listed at **http://www.fema.gov/authorized-equipment-list**.

2. **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**. 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

3. **Exercises:** Funding may be used to conduct **security-related exercises**. This includes costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, and documentation. Exercises afford organizations the opportunity to validate plans and procedures, evaluate capabilities, and assess progress toward meeting capability targets in a controlled, low risk setting.

4. **Training:** Nonprofit organizations may use NSGP funds for the following training-related costs:

   - Employed or volunteer security staff to attend security-related training within the United States;

- Employed or volunteer staff to attend security-related training within the United States with the intent of training other employees or members/congregants upon completing the training (i.e., "train-the-trainer" type courses);

- Nonprofit organization's employees, or members/congregants to receive on-site security training.

    - Allowable training-related costs: Costs are limited to attendance fees for training and related expenses, such as materials, supplies, and/or equipment.

    - Allowable training topics: Topics are limited to the protection of critical infrastructure key resources, including physical and cybersecurity, 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 organization's Investment Justification. Training should provide the opportunity to demonstrate and validate skills learned as well as to identify any gaps in these skills.

5. **Contracted Security Personnel:** The contracting of security personnel is an allowable cost under this program. The sub-applicant **must be able to sustain this capability** in future years without NSGP funding and **submit a sustainment plan** for the continued funding of this capability. Additionally, the State Administrative Agency my limit the percentage of the grant that may be budgeted for contracted security personnel. The funds may not be used to purchase equipment for contacted security. Some SAAs may require the submission of a sustainment plan at the time of application while others may require it post-award.

Generally unallowable/ineligible costs:

- **The development of risk/vulnerability assessment models**
- **Initiatives that fund risk or vulnerability security assessments or the development of the Investment Justification**
- **Reimbursement of pre-award security expenses**
- **Initiatives that do not address the implementation of programs/initiatives to build prevention and protection-focused capabilities directed at identified facilities and/or the surrounding communities**
- Organization costs, and operational overtime costs
- General-use expenditures
- Overtime and backfill
- Travel expenses
- Initiatives in which federal agencies are the beneficiary or that enhance federal property
- Initiatives which study technology development
- Proof-of-concept initiatives
- Initiatives that duplicate capabilities being provided by the Federal Government
- Organizational operating expenses

Note: All permissible costs to be considered for funding must be included in the Investment Justification within Part IV. Target Hardening. **If not included in this section, equipment, activities and contacted security will be ineligible for funding.** There are two parts to Part IV. to complete:

- A **narrative section** to describe all target hardening activities, as well as costs related to planning, exercises, training and contracted security personnel; and

- An **equipment identification section** that requires the input of details identifying the specific equipment (from the AEL list) to be acquired, including estimated costs. This part only pertains to equipment (and not the other categories of permissible costs, i.e., not training , planning or contacted security personnel.)

NSGP Investment Modifications to Change Scope or Objective: Requesting a change in the scope of an approved Investment Justification is **difficult and will likely lead to significant delays in project implementation**, as the original approval was based on a competitive process, with applications recommended for funding based on the threat, vulnerability, consequence, and mitigation specified in the IJ for a specified agency and location. Changes in scope or objective of the award require DHS/FEMA's prior written approval and will be considered on a case-by-case basis. As NSGP project funding is based on the ability of the proposed project to mitigate the risk factors identified in the IJ, **DHS/FEMA may reject requests to significantly change the physical security enhancements that are purchased with NSGP funding where DHS/FEMA believes approval of the request would change or exceed the scope of the originally approved project**. Nonprofit organizations with pending change of scope requests will not be permitted to proceed with implementing any scope/objective changes until the SAA receives written approval from DHS/FEMA and until the SAA has made any required subaward modifications. This could take several months before permission is granted.

Note: It is therefore advised that sub-applicants make certain that their initial IJ submissions include the scope of work they intend to pursue, if funded, and to avoid scope of work changes where possible.

The Secure Community Network (SCN): SCN provides several **training courses, tabletop exercises and related preparedness and training opportun**ities that may be funded with NSGP grant funds. Sub-applicants may want to contact SCN as they begin the planning process and with **assistance with risk/vulnerability assessments and critical infrastructure planning consultation**. For general inquiries and security consultation, you may contact SCN at: **dutydesk@securecommunitynetwork.org**. For training requests, you may SCN at: **training@securecommunitynetwork.org**.

Grant Application: Part V. Project Milestones

(This section is worth up to 4 points)

This section provides space for a sub-applicant to outline sequentially the expected key preparations, acquisition and installation milestones that allow them to reach its objectives

during the projects period of performance (i.e., the project schedule and scope of work)**.** Estimated start and completion dates must be provided for each milestone.

Note: In this section, **sub-applicants are asked to outline their "estimated" project implementation plan**. Completeness is important as the reviewers need to have confidence in the sub-applicant's full understanding of the scope of the project and what amounts to key milestones. The following serves as an example of a condensed list of milestones to illustrate ONLY what a sequence might look like. Each sub-applicant's response should be specific, complete, and relevant to their respective request and timeline.

Sample Sequence:

1. Receive award notification, complete award acceptance agreement, satisfy FEMA's **Environmental Planning and Historic Preservation review** (see below), and commence project.
2. Establish payment method and satisfy all financial and programmatic reporting requirements.
3. Hire vendors and contractors.
4. Order and acquire equipment.
5. Conduct engineering back work.
6. Install equipment.
7. Test equipment, develop punch list, and satisfy outstanding items and issues.
8. Train staff in use and maintenance of equipment and technologies.
9. Finalize delivery of project.
10. Schedule/conduct allowable training/exercises.
11. Close out project.

Note: As reference points, the anticipated period of performance will be 36-months. The period of performance will commence when the awards are noticed by FEMA around September 1, 2021 and no later than September 30th. The projected end-date is August 31, 2024. Regarding the milestone timeline, **a project cannot commence until prerequisite requirements of the acceptance agreement are met, including satisfying FEMA's Environmental Planning and Historic Preservation review and the State Administrative Agency gives the go-ahead.** This could take several months (i.e., 60-to-90 days or more) to complete. Therefore, the Milestone timeline should reflect this waiting period/delay.

Grant Application: Part VI, Project Management

(This section is worth up to 5 points)

The section sets forth senior management roles and responsibilities, governance structure and expertise required to successfully manage the project.

The following are three specific areas that need to be addressed:

1. **Provide project management details**, such as the complete contact information for the project manager, and a description of their relevant experience. To the degree known and applicable, a sub-applicant should also identify other persons who will be enlisted to advise, coordinate or help carry out the project, their expected roles, responsibilities and relevant experience.

Note: Where there are vacant positions or unknowns that are expected to be filled, then include each position to be filled and the expected roles, responsibilities, and qualifications for each position.

2. **Include a description of potential challenges to project implementation.** There may be known, foreseeable, and unknown challenges to implementing the project. The following are suggestions in how to respond:

    - Include any potential challenges identified in the risk assessment or by the project coordinator, or contactor for completing the project or aspects thereof.

    - There are a number of common or predictable challenges a sub-applicant should consider, including: delays in the notification of grant award; satisfactory completion of the administrative requirements for the release of funds (i.e., completion of financial and programmatic reports, compliance with Federal regulations, and other conditions of the award contract acceptance); delays in the acquisition of equipment and installation of same; changes in cost estimates or other planning assumptions.

    - A sub-applicant should include a blanket statement on the quality of its management and implementation team (quality controls) to minimize foreseeable and unforeseeable problems and to ensure that when challenges arise, they will be dealt with by experienced, competent and responsible professionals.

Note: All projects run into problems, delays, challenges. Sub-applicants should give real thought to what they might expect and convey a competence for handling them to a satisfactory conclusion.

3. **Describe coordination with State and local homeland security partners.** In addition to grant funding for target hardening and training activities or exercises, the NGSP grant opportunity is intended to promote a "Whole Community" approach to homeland security. In this section sub-applicants should **explain the intended improved integration of nonprofit security within broader State and local preparedness efforts. Suggestions**:

    - If a sub-applicant is collaborating with State and local homeland security partners on the grant project, they should include a description of the partnership, which might include assistance with conducting the risk/vulnerability assessment, conducting training and/or exercises through the grant and/or providing advice or materials in

furtherance of the grant. Whatever the engagement, it should be described in this section.

- If a sub-applicant has other interactions with State or local law enforcement outside of the grant, reference the relationship(s) in this section as well. This might include increased engagement or presence around high holidays or specific threat events/circumstances, or participation in emergency management training opportunities or drills.

- If a sub-applicant is not currently collaborating with law enforcement on the project, at a minimum they should incorporate an intention that they will reach out to their local law enforcement authorities/first responders during the implementation of their project, as a means of engagement and relationship building, and to elicit assistance and feedback to strengthen project outcomes. **This should be reflected in in both this and the Milestones section of the IJ**.

Grant Application: Part VII. Impact
(This section is worth up to 5 points)

In this section a sub-applicant is required to address two inquiries:

1. Explain the **expected measurable outputs and outcomes** derived from the completion of the project that would best illustrate the success of the project.

Note: The response should include a self-assessment (a statement) on how in practice the allocation of resources – the target hardening investments (set forth in Part IV) acquired through the grant -- most efficiently and effectively reduce the risks and vulnerabilities identified in the Risk sections (Part III) of the application and thus protect against the potential consequences of a potential terrorist attack.

2. Describe the security and resiliency posture that will be achieved through the grant. **This section will help DHS/FEMA assess the contributions the sub-applicant will make to national preparedness through the application of DHS/FEMA developed Core Capabilities descriptors** (critical mission areas).

Note: The risk/vulnerability assessment is used to prioritize resources to address the highest probability or highest consequence threats (i.e., terrorist attack). These resources are used to build or strengthen capabilities and activities implemented to best address those risks. In this section, sub-applicants should explain how the Investment/s they are requesting support building or sustaining one or more DHS/FEMA designated Core Capabilities through the grant. Think of core capabilities as the intended outcome/s or achievement/s (security posture) of the project, resulting from the investments made to address the threats and vulnerabilities assessed. Additionally, as national preparedness is considered interdependent, requiring a "Whole Community" approach, **it would be advisable to address how the outcomes and**

achievements (core capabilities) brought about through the grant might contribute to the greater resiliency/preparedness of other facets of the Whole Community: individuals/community/nonprofit sector/faith-based organizations/state/nation.

- Core Capabilities fall under one of the five following mission areas (buckets):

  - **Prevention:** *Avoid, prevent or stop an imminent, threatened or actual act of terrorism.*

    The Prevention mission area is composed of the capabilities necessary to avoid, prevent or stop a threatened or actual act of terrorism. It is focused on ensuring we are optimally prepared to prevent an imminent terrorist attack within the United States. Examples of Prevention Core Capabilities include: **Planning, Operational Coordination, and Screening and Detection.** (Some sub-applicants will conduct preparedness planning, training or exercises or acquire and install screening and detections equipment)

  - **Protection:** *Protect our citizens, residents, visitors, assets, systems and networks against the greatest threats and hazards in a manner that allows our vital interests and way of life to thrive.*

    The Protection Framework houses "the capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters." Examples of Protection Core Capabilities include: **Physical Protective Measures, Planning, Operational Coordination, Access Control and Identity Verification, Cybersecurity, and Screening and Detection.** (Most sub-applicants will be acquiring and installing one or more physical protective measures from section 14 or 15 of the Approved Equipment List)

  - **Mitigation:** *Reduce the loss of life and property by lessening the impact of disasters.*

    Mitigation is composed of "the capabilities necessary to reduce the loss of life and property by lessening the impact of disasters." Mitigation Core Capabilities include: **Planning, Operational Coordination, Long-Term Vulnerability Reduction, Risk and Disaster Resilience Assessment, and Threats and Hazards Identification.** (Every sub-applicant has conducted a risk/vulnerability assessment)

  - **Response:** *Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of an incident.*

    Examples of Response Core Capabilities include: **Planning, Operational Coordination, On-Scene Security, Protection, and Law Enforcement .** (Some sub-applicants are requesting contacted security personnel)

  - **Recovery:** *Assist communities affected by an incident to recover through a focus on the timely restoration, strengthening and revitalization of infrastructure, housing*

and the economy, as well as the health, social, cultural, historic and environmental fabric of communities affected by an incident.

Recovery is composed of the core capabilities necessary to assist communities affected by an incident to recover effectively. Examples of Recovery Core Capabilities include: **Planning, Operational Coordination, and Natural and Cultural Resources.** (Some sub-applicants may be cultural and social hubs of their communities, whose quick recovery from a threat or attack could be impactful on well-being of the community as a whole)

Note: For a complete overview of each capability go to:
https://www.fema.gov/media-library-data/1443799615171-2aae90be55041740f97e8532fc680d40/National_Preparedness_Goal_2nd_Edition.pdf

Bonus - Funding History

(This section is worth 5 points for sub-applicants who have not received a prior award)

Due to the competitive nature of the NSGP program (more applications than available funds), FEMA has applied a bonus between 1 – 10 points to the overall IJ score of sub-applicants who have not received a prior grant award. In FY 2020, 5 bonus points was applied. **All sub-applicants must set forth their NSGP funding history. Do not leave blank**.

Note: The amount of funding appropriated to the program in any given year may be a factor in the amount of bonus FEMA applies.

Applicant Contact Information

All IJ preparers must certify that they are either an employee or agent of the applying organization. **Be sure to check the box and provide name, e-mail address or phone number**. They will be the point of contact for the application, including award results.

Final Score

Congress appropriated $90 million for NSGP in FY 2020, directing $50 million to the Nonprofit Security Grant Program - Urban Area (NSGP-UA) and $40 million to Nonprofit Security Grant Program - State (NSGP-S). The funding levels for FY 2021 have not yet been determined.

Nonprofit organizations located within an UASI-designated urban area may only apply to NSGP-UA. Nonprofit organizations located outside of an UASI-designated urban area (everybody else) may only apply to NSGP-S. Both require a state and federal review. Once state and federal

reviewers score the sub-applications, they will be further weighted and prioritized according to the following factors:

- By a **factor of three** for nonprofit groups that are at a high risk of terrorist attacks due to their ideology, beliefs, or mission;
- By a **factor of two** for medical and educational institutions; and
- By a **factor of one** for all other nonprofit organizations.

Notes:

How an organization self-identifies itself will be a significant determining factor in the final score it will receive. It is, therefore, **incumbent upon ALL sub-applicants to make clear that their identity, work, beliefs, values, causes as identifiably Jewish communal institutions, makes them a high-risk target of attack by terrorists and domestic extremists because of their ideology, beliefs, or mission, so that their score is multiplied by a factor of three.** This should be validated in the sub-applicant's mission statement, risk/vulnerability assessment, and where applicable in the IJ, i.e., Parts I –III).

Additional Tips[3]

1. **Risk/Vulnerability Assessments:**

   - Conduct an informal self-assessment to familiarize yourself with potential security challenges for your facility. Consider your needs for situational awareness, site hardening, and incident response

   - Get an up to date, formal security assessment of the facility with a written report prepared by a community security director, regional security advisor, Secure Community Network, DHS Protective Security Advisor, state or local law enforcement, or other outside party. (A police crime prevention survey, self-assessment, or a guided assessment developed by an SAA may also suffice.) The most helpful documents are typically provided by independent and credentialed security professionals. The least helpful are often provided by vendors whose recommendations may not be objective.

   - Start early to find a quality assessor.

[3] With appreciation, the following security professionals contributed to developing these tips: **Robert M. Graves**, Regional Security Advisor for the National Capital Region; **Amy E. Keller**, Director of Security Initiatives and External Affairs, Jewish Federation in the Heart of New Jersey; and **David Pollock**, Associate Executive Director, and Director of Public Policy & Security, JCRC of New York.

2. **Vendors:**

   - Identify potential vendors or sources for products and services. Check with peers or local security advisors for reputable vendors.

   - Get two to three quotes for each product or service to estimate costs for your grant application. Ensure quotes include installation, maintenance, or service, as appropriate.

   - Discuss needed security measures with your organizational leadership to identify the most suitable solutions for the organization.

3. **State Administrative Agency:**

   - The SAAs have a fair amount of discretion and subjectivity in applying FEMA's grant guidance to their respective jurisdictions. It is therefore imperative that sub-applicants follow the guidance provided by their SAA (i.e., such key dates and deadlines, permissible costs, and state/jurisdiction pre-qualifications). There can be discrepancies between the federal guidelines and what the SAA requires.

4. **Drafting the IJ Response:**

   - Start to outline responses early so that there is time to refine the submission before the deadline.

   - Use a PC to complete the application. (Apple computer users have experienced technical problems with the application software.)

   - Minimize extraneous verbiage and focus on relaying the substance as concisely as possible. (Space to fill-in answers is limited in places.)

   - Check the math to make sure costs, numbers, figures are consistent throughout the IJ

   - Carefully read instructions before entering content into the Investment Justification. Responsiveness and completeness of the application is scored. **All questions in the IJ should be answered**. Partial credit is better than no credit. There is no room to lose points that can be earned.

   - It is critically important that the sub-applicant answer the questions asked within the sections/spaces where they appear. **No credit will be given for answers provided in the wrong sections/spaces**.

   - Leave time to test the IJ platform to ensure no last-minute technical glitches occur and that should problems arise they can be resolved before the submission deadline. Submit the IJ ahead of the deadline.

   - Review below check list before finalizing and submitting the IJ.

Important Check List

To ensure that the draft responses are as thorough and complete as possible, prior to finalization and submission of the IJ Investment form, review the following checklist:

1. **Has the sub-applicant contacted the State Administrative Agency to:**

    - Verify the state's application deadline?
    - Obtain information on any additional state requirements?

2. **Are the following components included in the application package?**

    - Mission statement
    - Vulnerability Assessment
    - Investment Justification (IJ)
    - Supporting documentation that substantiates threat, if applicable
    - Any other state required information

3. **Are the following items addressed within the IJ?**

    - Clearly identify risk, vulnerabilities, and consequences
    - Description of findings from a previously conducted vulnerability assessment
    - Details of any incident(s) that include description, dates etc.
    - Brief description of any supporting documentation such as police reports
    - Explanation of how the investments proposed will mitigate or address the vulnerabilities identified from a vulnerability assessment
    - Establish a clear linkage with the investment(s) and core capabilities re National Preparedness Goal
    - All proposed activities are allowable costs
    - Realistic milestones that consider such time-consuming requisites such as satisfaction of the Environmental Planning and Historic Preservation review
    - Description of the project manager's/team level of experience