The Jewish Federations® of North America
Washington Office

THE **STRENGTH** OF A PEOPLE.
THE **POWER** OF COMMUNITY.

Nonprofit Security Grant Program: Vulnerability/Risk Assessment

November 15, 2020

Point of Contact: Rob Goldberg, Senior Director, Legislative Affairs
Rob.Goldberg@JFNA.org

[Before proceeding, if you are a New York-based applicant, please 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. The below guidance is for all other applicants.]

Vulnerability/Risk Assessment

Overview

The NSGP provides funding support for hardening and other physical security enhancements to nonprofit organizations that are at high risk of terrorist attack. NSGP project funding is based on the ability of proposed projects to mitigate the risk factors identified in the applications (the Investment Justifications (IJ)). **Funded projects must be both feasible and effective at reducing the risks for which the projects were designed**.

The risk factors for which the IJ is based are derived from a vulnerability/risk assessment each NSGP project applicant is required to conduct and submit with the IJ to the SAA. NSGP projects are assessed based significantly on the ability of a proposed project to mitigate the risk factors identified in the IJ. **Past applicants who have recently conducted a risk/vulnerability assessment may rely on it again for FY 2021.** However, they will be limited to addressing the risks set forth in the previously conducted assessment. It is recommended that any **risk assessment more than two-years old be reevaluated or updated** to capture emerging risks and the corollary investments.

Note: An early priority of any nonprofit applying for the grant is to get a risk assessment completed, as it becomes the building block for developing the project and completing the IJ.

Vulnerability/Risk Assessment Preliminary Guidance

In making decisions, the determination of risk is a central factor in how the SAAs and FEMA rank and prioritize the applications they review. Therefore, each applicant must provide a Vulnerability/Risk Assessment, which serves as a framework for the applicant to use to identify risks and weaknesses and prioritize resources that address their most critical security needs.

Often **local police departments will conduct such an assessment, as do private companies**. Also, our colleagues at the **Secure Community Network (SCN) (and related community security directors and**

regional security advisors, as applicable) may be able to help, as described in Recommendation 3, below.

In practical terms the vulnerability/risk assessment is used to complete two sections of the application (IJ): Part III. Risk and Part IV. Target Hardening & Training. These sections address risk, vulnerability, and consequences of an attack and the recommend investments to mitigate them (See below under Investment Justification).

Note: A good vulnerability/risk assessment will identify any specific record of or relevant threat to the applicant and describe the vulnerabilities to be addressed through the grant award. It should spell out the specific protective measures required or recommended (whether target hardening, planning, training or exercises) that would most efficiently and effectively counter the risks, minimize the vulnerabilities and mitigate the potential consequences of an attack.

Recommendations

Recommendation 1 – Risk Assessor Should be Familiar with the IJ

Whoever is conducting the risk assessment, the applicant should make sure that assessor is familiar with (has a copy of) the IJ template, and, particularly, the Risk and Target Hardening & Training sections, and **designs or organizes the assessment report in a manner that is consistent with and helpful to completing the IJ**.

Note: A SAMPLE of the IJ is attached (it is for illustrative purposes only and should NOT be completed). Only the IJ posted with or at the time the FY 2021 Notice of Funding Opportunity commences should be used.

Recommendation 2 -- Emergency Planning & Training Activities should be Considered

Historically the NSGP has been restricted to purchases related to target hardening and physical security equipment. In recent years, funding allowances have expanded to place a priority focus on security-related training and other planning and preparedness activities, to include the development of emergency plans and procedures. As we have seen in past incidents and attacks, training and emergency response plans are some of the best investments organizations can make as part of a comprehensive physical-security program and have saved lives. As such, **we encourage applicants to include emergency planning and training activities as part of their grant applications.**

Note: Emergency planning and training activities need to be identified within the vulnerability/risk assessment if they are to be included in the IJ.

Recommendation 3 -- The Secure Community Network, Community Security Directors, and Regional Security Advisors may be Helpful

The Secure Community Network (SCN)[1] provides a range of services to assist organizations and facilities in support of the NSGP process. With respect to grant applications, **SCN provides assessments** as well as services in support of the application process. Post-grant award, SCN can provide technical information and advice. Additionally, SCN provides several training courses, tabletop exercises and related preparedness and training opportunities that may be funded with NSGP grant funds.

We encourage you to contact SCN as you begin your planning process and for assistance with assessments and critical infrastructure planning consultation. **Communities with local Community Security Directors or Regional Security Advisors, are encouraged to connect directly with those dedicated resources.**

Note: Due to the volume of requests during grant season, SCN can conduct a limited number of assessments on a first-come, first-serve basis. For General Inquiries & Security Consultation, individuals may contact SCN by email (dutydesk@securecommunitynetwork.org) or by phone 844.SCN.DESK to be connected with SCN security experts. For Training Requests, individuals may inquire about trainings, or to schedule one for their community and/or facility, please contact our Training Desk via email at training@securecommunitynetwork.org.

Recommendation 4 -- Assessment Tools

There may be circumstances where a sub-applicant will choose to conduct a self-assessment, or a local law enforcement agency or vendor may not have a good assessment tool of their own. In these cases, the following self-assessment resources may be employed in carrying out the Vulnerability/Risk Assessment:

Self-assessment tools:

1. The Secure Community Network has adapted this Facility Assessment tool from best practice examples to aid non-profits, community organizations and related facilities in identifying areas of site security concerns.
Link: https://mcusercontent.com/0b3c7e1421bd2734b0610a1fb/files/c4ca3b0c-7163-40bd-a3d9-ca3268765054/SCN_Facility_Self_Assessment_Document_Sept_2019_1_.pdf

2. Potential Indicators, Common Vulnerabilities, and Protective Measures: Religious Facilities.
Link: https://www.jcrcny.org/wp-content/uploads/2017/03/CVPIPM_Religious-Facilities_PSCD.pdf

3. Emergency Preparedness Planning Guide for Childcare Centers. From the Illinois Emergency Medical Services for Children (a collaborative program between the Illinois Department of Public Health and Loyola University Chicago). Lots of ideas to keep toddlers safe.
Link: https://www.jcrcny.org/wp-content/uploads/2016/10/Emergency-Preparedness-Planning-Guide-for-Child-Care-Centers.pdf

[1] SCN is a non-profit organization that serves as the official safety and security organization of the Jewish community in North America, working under the auspices of The Jewish Federations of North America and the Conference of Presidents of Major American Jewish Organizations.

4. Readiness and Emergency Management for Schools (REMS) Technical Assistance Center, U.S. Department of Education.
Link: https://rems.ed.gov/AboutUs.aspx?AspxAutoDetectCookieSupport=1

5. REMS: Conducting a School Safety Audit.
Link: https://rems.ed.gov/docs/repository/00000379.pdf

6. California STAS: Protective Measures for Enhanced Facilities Security.
Link: https://www.jcrcny.org/wp-content/uploads/2015/01/141104-FOUO-STAS-Protective-Measures-for-Enhanced-Facility-Security-.pdf

7. New Jersey Office of Homeland Security and Preparedness Critical Infrastructure Protection Bureau: Facility Self-Assessment Tool Develop effective answers.
Link: https://www.jcrcny.org/wp-content/uploads/2018/06/NJ-FacilityAssessmentTool5.25.17.pdf