INDIANA NONPROFIT SECURITY GRANT PROGRAM (IN-NSGP)
VULNERABILITY ASSESSMENT

INFORMATION:

Application for the Nonprofit Security Grant Program (NSGP) requires the submission of a Vulnerability Assessment (VA) as part of the application package. Assessments should cover such general areas as threats, vulnerabilities and mitigation options, consequences, perimeter, lighting and physical protection, etc.

This template is based on requests from applicants needing assessment guidance. The use of this template is not mandatory, but if an applicant chooses to use this Vulnerability Assessment template, please complete and return it with your grant application.

Assessors and applicants should collectively discuss security-related questions during the assessment phase of the VA. This inclusive approach will help the applicant complete the grant application and help the nonprofit organization become more aware of the risks to its facility and members.

VULNERABILITY ASSESSMENT:

When possible, the vulnerability assessor(s) for the NSGP grant should coordinate with local law enforcement, security or safety representatives to get a clear picture of potential threats, risks or attacks to the nonprofit organization's facility or members.

For the purpose of the NSGP grant, the vulnerabilities identified in this assessment need to be tied to terrorism on the Investment Justification (IJ) Form.

Terrorism is defined as any activity that involves an act that is dangerous to human life or potentially destructive of critical infrastructure or key resources. It also appears to be intended to intimidate or coerce a civilian population, influence a policy of a government by intimidation or coercion or affect the conduct of a government by mass destruction, assassination or kidnapping. (18 U.S.C. § 2331(5))

FACILITY AND ASSESSOR INFORMATION:

Organization Name:	
Organization Physical Address:	

Section 1 – Assessor Information	
Assessment Conducted By: (Select one from dropdown menu)	Click down arrow to select: Choose an item
If "Other," please describe:	
Name of Assessor:	
Title of the Assessor:	
Date of Assessment:	

The following sections collect deficiencies regarding the vulnerability to potential threats, risks or attacks to the nonprofit organization's facility or to its members. **Just a reminder, these deficiencies and vulnerabilities need to be tied to terrorism on the FEMA Investment Justification (IJ) Form**.

Section II - Perimeter Control	Describe Deficiencies and Vulnerabilities
Does the facility have a clearly defined perimeter or boundary?	
Does the site have a well-established perimeter using natural materials or fencing/walls?	
Are there deficiencies in the security perimeter?	
Does the organization effectively address all vehicle and pedestrian entry and exit points?	
Does the facility have barriers to reduce high-speed avenues of approach?	
Is the perimeter checked routinely by staff, volunteers, members or security?	

Section III – Access and Entry Control	Describe Deficiencies and Vulnerabilities
Does the interior layout of the facility provide escape routes for effective emergency egress/exits?	

Do exterior double doors have handles that can be tied or chained together to prevent emergency evacuation or access by first responders?	
Is there an effective entry control system, visitor pass/badge system, or visitor escort policy and/or procedure?	
Does the facility have sufficient signage both inside and outside?	
Does the construction of exterior doors and windows deter or delay an attack?	
Can facility doors be easily closed and locked to prevent access from an intruder?	

Section III - Security Lighting	**Describe Deficiencies and Vulnerabilities**
Are all doorways and pathways illuminated for security, safety and assistance with movement?	
Is the lighting adequate to assist the security camera system to detect and identify activities?	

Is the lighting adequate in critical areas? (i.e., at roadway access and parking areas)	

Section IV – Camera/Intrusion Detection	**Describe Deficiencies and Vulnerabilities**
Is there an intrusion detection system installed? (security camera system, motion sensors, door and/or window alarms, etc.)	
Is the intrusion detection system monitored? (i.e., on-site, off-site, mobile)	
Does the facility's security systems directly communicate with local law enforcement?	
Is information recorded and reviewed?	
Section V - Security Operations	**Describe Deficiencies and Vulnerabilities**
How does the organization communicate with employees and members during emergencies?	
Does the facility use a security company, employees, volunteers or members to perform security patrol operations?	
Are there plans, policies and/or procedures for the facility's security activities? (i.e., facility access or badging procedures, reporting suspicious activities or individuals, active shooter actions, security logs, how to address unattended vehicles)	

Other vulnerabilities not listed on assessment:	

Section VI – Vulnerabilities To Be Addressed

This section helps the applicant prioritize vulnerabilities and select facility hardening (equipment and/or activities) options to complete the investment justification. Not all vulnerabilities identified during the assessment are critical to the operation of the nonprofit site and may not be listed.

This section is used to validate requests for specific equipment or other facility hardening activities in Part IV of the current application (FEMA IJ Form) for grant.

Prioritize the most critical vulnerabilities that could be exploited through acts of terrorist actions and/or threats directed at the nonprofit facility and/or organization. Also, provide facility hardening options including equipment/activity investments and potential consequences for vulnerabilities. This data will assist the grant applicant to identify the vulnerabilities and consider target hardening options to complete the investment justification.

Vulnerability:

Facility Hardening/Investment (equipment):

Vulnerability:

Facility Hardening/Investment (equipment):

Vulnerability:

Facility Hardening/Investment (equipment):

Vulnerability:

Facility Hardening/Investment (equipment):

Vulnerability:

Facility Hardening/Investment (equipment):

Vulnerability:

Facility Hardening/Investment (equipment):

Vulnerability:

Facility Hardening/Investment (equipment):

Vulnerability:

Facility Hardening/Investment (equipment):

Vulnerability:

Facility Hardening/Investment (equipment):