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

INFORMATION

The 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.

This template is based on requests from applicants needing assessment guidance. The use of this template is not mandatory, but if you choose to use this VA form, 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 the site and members.

Organization Name	
Organization Physical Address	

Assessor Information	
Assessment Conducted By (Select one from dropdown menu)	Choose one... Click Here
If Other was selected, please describe.	
Name of Assessor and Any Associated Credentials (Examples: CPP, PSP, CTM, TLO, military or other security, inspection or auditing credentials)	
Signature of the Assessor	
Date of Assessment	

Threat Assessment

When possible, the vulnerability assessor(s) for the grant should coordinate with local law enforcement and/or Urban Area Security Initiative (UASI) representatives to get a clear picture of the current threats from terrorism to the nonprofit organization members and site.

For the purpose of the grant, terrorism is defined as human-caused threats against persons or property to achieve political or social objectives.

Overall Description of Threat(s)	
List any acts of terrorism against persons or property directed at the nonprofit site initiated to achieve political or social objectives during the last five years. Attach any photos, news articles or police reports that validate the incidents.	
Incidents	**Describe the Impact to the Nonprofit Site**
1	
2	
3	
4	

(Attach additional document if more lines needed.)

This section is provided to assist assessors and applicants with collecting security-related data on the nonprofit organization and site. Your submission should cover the same general areas such as threats, vulnerabilities and mitigation options, consequences, perimeter, lighting and physical protection.

Nonprofit - Perimeter and Access Control Assessment	
Does the facility have a clearly defined perimeter? Is this perimeter boundary posted? **(Yes or No - Describe if appropriate.)**	
Does the site have perimeter fencing, and is this fencing maintained? Is the perimeter fence clear of vegetation and debris? Do you have a clear line of site through the perimeter fence? **(Yes or No - Describe if appropriate or attach photos.)**	
Are there known deficiencies in the security perimeter? Are deficiencies being corrected? What is the status? **(Yes or No - Describe if appropriate or attach photos.)**	
Are Intrusion Detection System (IDS) sensors integrated into perimeter property line protection? **(Yes or No - Describe if appropriate.)**	
Does the organization effectively address all vehicle and pedestrian entry and exit points? Does the site, facility or installation have high-speed avenues of approach? **(Yes or No - Describe if appropriate.)**	

Does the site, facility or installation have illumination at any or potential security checkpoints to examine credentials, personnel and vehicles? **(Yes or No - Describe if appropriate.)**	
Is the perimeter checked routinely by staff, volunteers, members or security? **(Yes or No - Describe if appropriate.)**	

Nonprofit - Security Lighting	
Are doorways illuminated for security and safety? **(Yes or No - Describe if appropriate.)**	
Are pathways around the site illuminated to assist with movement and safety? **(Yes or No - Describe if appropriate.)**	
Is the lighting adequate to assist the security camera system to detect and identify activities around the site? **(Yes or No - Describe if appropriate.)**	
Are all identified critical areas covered by lights? Is the lighting adequate from a security perspective at roadway access and parking areas? **(Yes or No - Describe if appropriate.)**	
Does vegetation or debris obstruct illumination or create dark shadows? **(Yes or No - Describe if appropriate.)**	

Nonprofit - Security Intrusion Detection, Security Camera System, Fire System	
Does the site, facility or installation have a security center? Does the center have adequate access control and alarm procedures? Is the center highly visible, and has a secondary center been identified if the first one is affected by an incident? **(Yes or No - Describe if appropriate.)**	
Does the site have an operational intrusion detection system (IDS) installed on all windows, doors, skylights, crawl spaces and roof hatches? **(Yes or No - Describe if appropriate.)**	
Does the IDS provide any specific or more focused coverage of identified critical assets? **(Yes or No - Describe if appropriate.)**	
Does the site have a security camera system in place? **(Yes or No - Describe if appropriate.)**	

Are all facility critical assets under security camera system coverage? **(Yes or No - Describe if appropriate.)**	
Are the security camera feeds or IDS systems monitored? (e.g., on-site, off-site, mobile) **(Yes or No - Describe if appropriate.)**	
Are the security cameras and IDS sensors integrated in order to detect, identify and respond to alarm activations? **(Yes or No - Describe if appropriate.)**	
Does the physical security protection system integrate the lights, cameras, fire alarms and other sensors into a manageable security system? **(Yes or No - Describe if appropriate.)**	
Do the facility's systems directly communicate with local law enforcement and fire? **(Yes or No - Describe if appropriate.)**	
Nonprofit - Security Operations	
Does the facility use a security company, employees, volunteers or members to perform security patrol operations? **(Yes or No - Describe if appropriate.)**	
Are entry control visual inspections evident at entry points? **(Yes or No - Describe if appropriate.)**	
Are after-hours checks made of the facility by employees, volunteers or members? **(Yes or No - Describe if appropriate.)**	
Are the observations of the patrol documented in a daily security log? **(Yes or No - Describe if appropriate.)**	
Are there procedures for reporting suspicious personnel or activities? **(Yes or No - Describe if appropriate.)**	
Is there an effective employee entry control badge system, visitor pass system or visitor escort policy and procedure? **(Yes or No - Describe if appropriate.)**	
How does the nonprofit organization communicate with employees, volunteers and members during emergencies? **(Describe.)**	

Nonprofit - Vulnerability Assessment Attachment List (e.g., photographs, maps, diagrams)

(Attach additional document if more lines needed.)

Mitigation Options

This section helps the applicant identify vulnerabilities, consider potential consequences and select target hardening (mitigation) 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. Mitigation options and consequences should be listed with the vulnerabilities. This section is used to validate requests for specific equipment in the current application for grant.

List the vulnerabilities that could be exploited through acts of terrorism/threats directed at the nonprofit site/organization. Also, provide a mitigation option and potential consequences for vulnerabilities. This data will help identify the vulnerabilities and consider target-hardening options to complete the investment justification.
Vulnerability Mitigation Options (target hardening)
Vulnerability Mitigation Options (target hardening)

(Attach additional document if more lines needed.)