EXAMPLE OF COMPLETED ASSESSMENT

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.

IDHS created this template 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:	XYZ Non-Profit Agency
Organization Physical Address:	123 Main Street Hoosier, Indiana 44444

Section 1 – Assessor Information	
Assessment Conducted By: (Select one from dropdown menu)	Click down arrow to select: Local Law Enforcement
If "Other," please describe:	
Name of Assessor:	Johnnie B. Good
Title of the Assessor:	Patrol Sergeant, Hoosier Indiana Police Department
Date of Assessment:	2/5/2025

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?	No. There is a sidewalk along 2 sides of the building and parking lot and an organization sign. However, at the back end of the parking lot, there is a gravel area that flows over into a vacant lot. Not having a clearly defined perimeter allows for unauthorized entry onto the facility's property and increases the risk of threats to staff, visitors, facility assets and vehicles.
Does the site have a well-established perimeter using natural materials or fencing/walls?	No. This vulnerability leaves the facility at risk for unauthorized entry and increases the risk to staff, visitors, facility assets and vehicles from threats.
Are there deficiencies in the security perimeter?	Yes. The facility does not have any camera system in place to see who is on the grounds or wants access to the facility. This vulnerability leaves the facility at risk for unauthorized entry and increases the risks to personnel, visitors, and facility assets from potential threats.
Does the organization effectively address all vehicle and pedestrian entry and exit points?	No. The facility has no formal process for addressing how vehicles gain access to the parking lot or the facility. There is no signage directing guests as where to enter and sign in. They do have a secretary that sits in an office inside the front entrance of the building but does not see who enters the building until they are at her doorway. These vulnerabilities leave the facility at risk for unauthorized entry.
Does the facility have barriers to reduce high-speed avenues of approach?	No. The facility has a large parking lot and has no building barriers to slow down vehicles. The vulnerability is a deliberate or accidental vehicular impact or explosion including targeting the building and occupants.
Is the perimeter checked routinely by staff, volunteers, members or security?	No. Staff only check the parking lot when arriving and leaving the facility. There is no policy, plan, procedure or training for staff to conduct security sweeps. Having no policies, procedures, plans, training or exercises leaves the staff without the basic skills to properly protect themselves and other occupants inside and outside the building and protect the facility's critical assets.

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?	No. There is no signage in the facility displaying proper emergency egress. This creates a dangerous and potentially deadly situation should occupants need to evacuate quickly.
Do exterior double doors have handles that can be tied or chained together to prevent emergency evacuation or access by first responders?	Yes. The front entrance double doors are able to be chained or tied together. This creates a dangerous and potentially deadly situation should occupants need to evacuate quickly, or first responders need entrance to the front entrance.
Is there an effective entry control system, visitor pass/badge system, or visitor escort policy and/or procedure?	No. There is no system or process for granting access to the parking lot or the internal facility. These vulnerabilities leave the facility at risk for unauthorized entry.

Does the facility have sufficient signage both inside and outside?	No. There is insufficient signage posted on and around the facility. The exterior facility doors are not marked. Unmarked doors make it difficult for first responders to identify and reference locations/rooms during an emergency, contributing to confusion and/or delayed response times. Moreover, absent or limited signage can diminish intruder deterrence, confuse visitors, fail to advise of specific hazards and hinder emergency evacuation efforts.
Does the construction of exterior doors and windows deter or delay an attack?	No. The facility's main entrance door lacks sufficient access control, enabling unauthorized entry from outside the facility. All doors and windows are original to the facility. The main entry double door and is metal and has a full window on both doors but is not reinforced. The other external doors are without windows. All windows are wood. The antiquated doors and windows make the facility more susceptible to unauthorized or undetected entry. Multiple access points are difficult to monitor and make proper access control challenging. Efforts to secure the facility in a lockdown situation may be delayed.
Can facility doors be easily closed and locked to prevent access from an intruder?	No. The main door to the facility is a double door that is always open during business hours, but the windows and other exterior doors are locked. The locks on all exterior doors are key-based locks. The internal doors, including meeting rooms, are normally left open. Staff often will prop open exterior doors while they go outside to smoke or take breaks. These vulnerabilities leave the facility at risk for unauthorized entry.

Section III - Security Lighting	Describe Deficiencies and Vulnerabilities
Are all doorways and pathways illuminated for security, safety and assistance with movement?	No. The only lighting is what is reflected from inside the facility. This vulnerability increases the risk of accidental injury and promotes criminal or vagrant activity in the area. Additionally, limited lighting along the building leaves the facility at risk for unauthorized entry and may impact access control procedures.
Is the lighting adequate to assist the security camera system to detect and identify activities?	No. There are no security cameras located outside or inside the facility. Inadequate lighting may render surveillance equipment ineffective, creating gaps in the facility's monitoring ability and leave the facility at risk for unauthorized entry.
Is the lighting adequate in critical areas? (i.e., at roadway access and parking areas)	No. The only lighting is what is reflected from inside the facility. This vulnerability increases the risk of accidental injury and promotes criminal or vagrant activity in the area. Additionally, limited lighting along the building leaves the facility at risk for unauthorized entry and may impact access control procedures.

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.)	No. There are no cameras or intrusion detection systems installed inside or outside the facility. This vulnerability increases the ability to detect suspicious activities and respond to a threat. This may delay and expose staff and facility assets to risk. Furthermore, inadequate security camera coverage may also hinder the efficiency of a post-incident investigation.
Is the intrusion detection system monitored? (i.e., on-site, off-site, mobile)	No. There is no intrusion detection system in place. Inadequate cameras and alarm sensors leave the facility at risk for unauthorized entry and may impact access control procedures.
Does the facility's security systems directly communicate with local law enforcement?	No. There is no intrusion detection system in place. Inadequate cameras and alarm sensors that are unable to communicate with local enforcement leave the facility at risk for unauthorized entry and may impact access control procedures.
Is information recorded and reviewed?	No. There is no intrusion detection system in place. Inadequate cameras that record leave the facility at risk for unauthorized entry and may impact access control procedures.
Section V - Security Operations	**Describe Deficiencies and Vulnerabilities**
How does the organization communicate with employees and members during emergencies?	There is no mass notification or alarm system in place to alert staff and occupants inside the building. The lack of communication or notification may lead to an increase of injuries or deaths during an attack.
Does the facility use a security company, employees, volunteers or members to perform security patrol operations?	No. There are no security patrol operations in place. The vulnerability of this leaves the staff without the basic skills to properly protect themselves and other occupants inside and outside the building and protect the facility's critical assets.
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)	No. Having no policies, procedures, plans, training or exercises leaves the staff without the basic skills to properly protect themselves and other occupants inside and outside the building and protect the facility's critical assets.
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: Perimeter Fencing

Facility Hardening/Investment (equipment) Install a 6' perimeter fence with an entrance gate equipped with proper access control hardware. The locked gate will be installed with a reprogrammable code key and a remote access intercom and camera.

Vulnerability: Structural Door and Window Weakness

Facility Hardening/Investment (equipment) Install 2 bullet-resistant main entrance doors with non-closed loop handle alternatives. Install 5 new exterior doors with metal doors. Install unprotected shatter resistance glass with security film on the 2 main entrance doors and 10 facility windows.

Vulnerability: Vehicle Standoff Distance from Facility

Facility Hardening/Investment (equipment) Install 10 vehicular barriers bollards in front of and the side of the facility to keep vehicles at a safe distance from building and reduce the impact of a potential vehicle-borne improvised explosive device (VBIED).

Vulnerability: Insufficient Camera and Intrusion Detection

Facility Hardening/Investment (equipment) Install 15 recording security cameras and 20 motion sensors to monitor activity inside and outside the facility. Install 5 exterior doors with an alarm providing an audible indication if opened or left ajar.

Vulnerability: Insufficient Exterior Lighting

Facility Hardening/Investment (equipment) Install 3 parking lot lights and 10 affixed lights around building, including 6 lights for exterior doors and 4 additional lights strategically placed on building.

Vulnerability: Mass Communication System

Facility Hardening/Investment (equipment) Purchase 4 handheld two-way radios enabling communication before, during, and after an emergency situation. Install 2 panic buttons in a concealed location. The button can send a silent emergency notification to an alarm company or law enforcement agency, indicating the source and location of the alert.

Vulnerability: Insufficient Signage

Facility Hardening/Investment (equipment) Purchase and post 25 signs inside facility, 15 signs outside facility and 6 internal and external door signs. Signs will display such information as door numbers, emergency evacuation instructions, traffic regulations, pedestrian flow and safety hazards. Signage will be concise, legible from a distance and well-lit.

Vulnerability: Security and Access of Facility Doors

Facility Hardening/Investment (equipment) Install electronic access control systems for main entrance door and 5 other exterior doors.

Vulnerability: Security Plans, Policies or Procedures

Facility Hardening/Investment (equipment) Hire a contractor to assist the facility in developing a Facility Emergency Operations Plan, policies and Standard Operating Procedures (SOPs) and checklists. Upon completion, train and exercise staff to ensure procedures are understood and staff are able to implement.

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)