FISCAL YEAR 2024
NONPROFIT SECURITY GRANT PROGRAM
PREAPPLICATION WEBINAR

Mr. Jason Guthaus
Mr. Paul Lounsberry

GOALS TODAY

Goals for this webinar:

1. Have a better understanding of the application process.

2. How to submit the application.

3. Gain knowledge of what might be asked of the organization if awarded.

- A copy of this PowerPoint will be sent out.

- Please mark down any questions you have - we will have time at the end to answer them.

- Mics and cameras have been muted at this time to avoid audio feedback.

- Mics will be turned on during question and answers at the end.

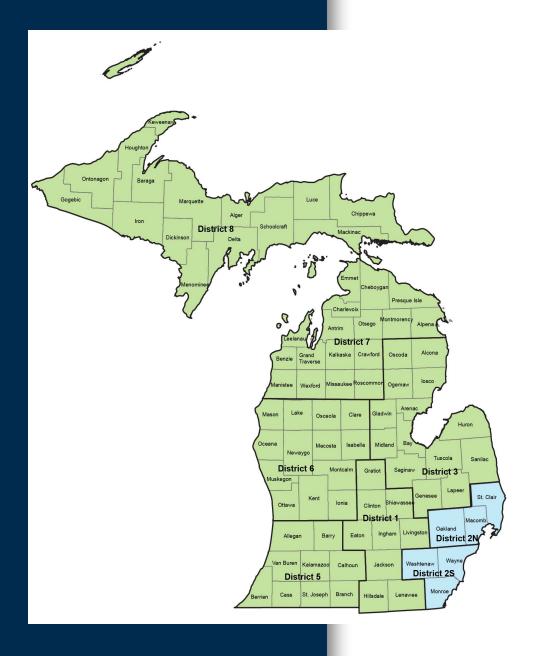# WHAT IS THE NONPROFIT SECURITY GRANT PROGRAM (NSGP)?

The Nonprofit Security Grant Program (NSGP) is a federal grant program offered through the Federal Emergency Management Agency (FEMA) and administered in Michigan by the Michigan State Police, Emergency Management and Homeland Security Division (MSP/EMHSD) that provides funding support for target hardening and other physical security enhancements to nonprofit organizations that are at risk of a terrorist attack.

- Highly competitive.
- Reimbursement- based.
- 36-month period of performance.

WHO IS ELIGIBLE TO APPLY?

___

The State Administrative Agency (SAA) is the only entity eligible to apply to FEMA for NSGP funding on behalf of an eligible nonprofit organization. Nonprofit organizations must apply to their SAA as the sub-applicant.

- Nonprofit Security Grant Program Urban Areas (NSGP-UA): To qualify for this program you must be in FEMA-designated urban area.

- Nonprofit Security Grant Program Statewide (NSGP-S): This program includes all organizations outside the FEMA-designated urban area.

GRANT TIMELINE

Grant money is appropriated by Congress.

The FEMA has 60 days to release the Notice of Funding Opportunity (NOFO).

Within 60 days after the release of the NOFO the SAA submits scored and prioritized applications to FEMA.

The nonprofit must complete the investment justification and submit the application packet to EMHSD.

The EMHSD verifies the application packets are complete and provides the applications to the scoring groups for scoring.

Scoring groups score and prioritize the applications.

The EMHSD prepares the applications for submission to FEMA.

APPLICATION DOCUMENTS

The following is required in the application packet:

1. Nonprofit Security Grant Program (NSGP) Investment Justification (Application);

2. Vulnerability Assessment;

3. Contact Info Sheet;

4. Executive Compensation;

5. Mission Statement.

The next couple slides we will dive into each document.

Nonprofit Security Grant Program (NSGP) (michigan.gov)

NONPROFIT SECURITY GRANT PROGRAM INVESTMENT JUSTIFICATION

APPLICATION DOCUMENT #1

INVESTMENT JUSTIFICATION

Reduction Project (1660-0110) NOTE: Do not send your completed form to this address.

PART I. NONPROFIT ORGANIZATION SUBAPPLICANT INFORMATION				
Identify the following:				
LEGAL NAME OF THE ORGANIZATION				
Made Up Organization United				

Please list the physical address of the facility. *One investment justification per facility.*	STREET			
	Make Believe Street			
	CITY	STATE	ZIP CODE	COUNTY
	Not Real	MI	12345	Example County

Please enter the year the facility listed above was constructed:	1900	

Is the building owned, or are you leasing/renting?	*If leasing or renting, do you have the owner's permission to make the proposed security enhancements?* ☒ Yes ☐ No
Rent/Lease ▾	

What year did you begin operating in/from this facility/building?	1920	

INVESTMENT JUSTIFICATION (CONTINUED)

Are you the only nonprofit operating in/from this facility/building? ☒ Yes ☐ No

If "No," please explain how the proposed security enhancements benefit both you and the other organization(s).

Note: Only one nonprofit can apply per building/facility/physical structure/address. However, the request and subsequent security enhancements may benefit nonprofits who cohabitate/operate in/from the same location. Multiple requests for federal assistance from the same physical address/building/facility/structure will all be deemed ineligible.

Based on your mission statement, please summarize your organization's mission, ideology, and/or beliefs.

Our Vision
Be a leader and partner in law enforcement and public safety, with a highly trained, full-service state police force that is mobile, flexible, and responsive to emerging public safety needs across Michigan.

Our Value Statement
"A PROUD tradition of SERVICE through EXCELLENCE, INTEGRITY, and COURTESY"

What is the primary organization type? Other ▼

If "Other," please describe the type of organization.

Example

Please select the organization's primary affiliation:	Other	▼

If "Other," please describe affiliation.

Example

Eligible organizations are registered 501(c)(3) nonprofits or otherwise are organizations as described under 501(c)(3) of the Internal Revenue Code (IRC) and tax-exempt under section 501(a) of the IRC. More information on tax-exempt organizations can be found at: https://www.irs.gov/charities-non-profits/charitable-organizations.

Is the organization eligible under the IRC to receive NSGP funds?	☐ Yes	☐ No

Does the organization have a Unique Entity ID (UEI) Number?	☐ Yes	☐ No

If "Yes," please enter the UEI Number for the organization:

Applications can only be submitted with a current and valid UEI number; pending UEI numbers will not be accepted.

Are you physically located in a current Urban Area Security Initiative designated urban area?	☐ Yes	☐ No

If "Yes," select the designated urban area from the list ▼

Total federal funding requested under the NSGP (will automatically populate based on entries in Section IV-B):

INVESTMENT JUSTIFICATION (CONTINUED)

PART II. BACKGROUND INFORMATION (5 POSSIBLE POINTS OUT OF 40)

Please describe (if applicable) this location's symbolic value as a highly recognized national or historic institution/landmark that renders the site as a possible target of terrorism.

The White House stands for freedom and democracy. It is also a symbol of our president, our country's history, and the American people. More than 200 years ago, the United States was a brand-new country and many people thought it might be a good idea to have a central place where the president would live and work, which led to the creation of The White House. Every year millions of people visit The White House. As such a prominent and important part of American history and democracy The White House would be a potential target of terrorism. There is the possibility for a high number of causalities and the publicity of an attack on The White House would cause fear across the entire nation.

Please select (if applicable) the current, ongoing, or recent (last 3 years) event(s) in which your organization has been involved in prevention, protection, response, and/or recovery:

Please describe the organization's role in prevention, protection, response, and/or recovery, specifically highlighting the efforts that demonstrate integration of nonprofit preparedness with broader state and local preparedness efforts.

Our organization could have a significant role in responding to and recovering from terrorist attack. It is stocked with food and water and has a back up power supply. It can be used as a shelter, and even has a full kitchen and areas in which to shower and wash clothes if long term sheltering is needed. There are several roads that can be used to access the organization and it is unlikely to be cut off from the rest of the community. Our organization is part of the community VOAD.

INVESTMENT JUSTIFICATION (CONTINUED)

PART III. RISK (15 POSSIBLE POINTS OUT OF 40)
Department of Homeland Security defines risk as the product of three principal variables: Threat, Vulnerability, and Consequence. In the space below, describe the risk(s) faced by your organization specifically in terms of the A) Threats, B) Vulnerabilities, and C) Potential Consequences of an attack.
A) Threat: In considering a threat, please describe the identification and substantiation of specific threats or attacks against the nonprofit organization or a closely related organization, network, or cell. *Description can include findings from a threat or risk assessment, police report(s), and/or insurance claims specific to the location being applied for including dates of specific threats.*
First include information from specific incidents at your facility including police reports, and/or insurance claims. Next, identify terrorist-related threats and hazards based on events at similar or nearby facilities including active shooters, attacks using sharp-edged weapons, explosive devices, arson, mail and package attacks, and vandalism. Which are most likely to occur, and which will cause the most serious consequences?
B) Vulnerabilities: Please describe the organization's susceptibility to destruction, incapacitation, or exploitation by a terrorist attack.
Summarize the gaps found in your completed vulnerability assessment. Ensure to identify which vulnerabilities lead to a higher probability of an attack or larger consequences in the event of an attack. Be specific and do not be afraid to pull language exactly from your vulnerability assessment.
C) Potential Consequences: Please describe the potential negative effects on the organization's assets, systems, and/or function if damaged, destroyed, or disrupted by a terrorist attack.
Explain the potential consequences of a terrorist attack on your facility. Be sure to include the potential for loss of life, loss of property, potential for mass casualties (if applicable), loss of reputation, impact on community, and any other foreseeable consequence.

INVESTMENT JUSTIFICATION (CONTINUED)

PART IV. FACILITY HARDENING (9 POSSIBLE POINTS OUT OF 40)

Section IV-A: In this section, describe each proposed activity or investment (as selected in Section IV-B), identify the vulnerability that it addresses, and detail the cost associated with the activity or investment. For each activity/investment, include the quantity, estimated hourly rate or estimated price per unit, and proposed usage.
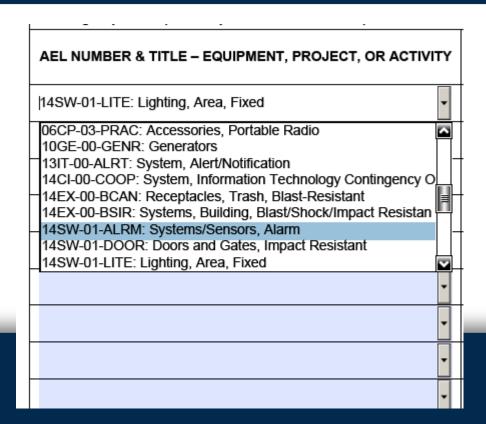
Allowable costs include facility hardening activities, such as planning and exercise related costs, contracted security personnel, and security-related training courses and programs limited to the protection of critical infrastructure key resources. Funding can also be used for the acquisition and installation of security equipment on real property (including buildings and surrounding property) owned or leased by the nonprofit organization, specifically in prevention of and/or in protection against the risk of terrorist attack.

On page 16 of our completed vulnerability assessment a risk of unauthorized access to our facility has been identified. There is currently no way to monitor whether a door is locked or unlocked other than walking and checking each door. Doors can be unlocked from the inside and left unlocked without detection and could provide an easy entrance for an active shooter. The current doors are also old and easily broken through. In order to address this identified vulnerability, we want to install a physical access control system (14SW-01-PACS), impact resistant doors (14SW-01-DOOR), and an alarm system (14SW-01-ALRM) to ensure there is no unauthorized access to the facility. The system will include impact resistant doors with automatic locking mechanisms, an alarm that rings when a door is propped open, and a video intercom system will be installed to allow authorized guests access.
14SW-01-PACS- $30,000 14SW-01-DOOR- $25,000 14SW-01-ALRM- $15,000

INVESTMENT JUSTIFICATION (CONTINUED)

Section IV-B: In this section, list all proposed facility hardening equipment, projects, or activities as allowable per the Authorized Equipment List (AEL), NSGP Notice of Funding Opportunity (NOFO), and Preparedness Grants Manual (PGM). Select the AEL number and title, list the vulnerability the equipment/project/activity addresses, and enter the estimated funding requested (round up to the nearest dollar).

AEL NUMBER & TITLE – EQUIPMENT, PROJECT, OR ACTIVITY	VULNERABILITY TO BE ADDRESSED	ESTIMATED FUNDING REQUESTED (Round to nearest dollar)
14SW-01-ALRM: Systems/Sensors, Alarm	Unauthorized Entry Pg 16	$15,000
14SW-01-DOOR: Doors and Gates, Impact Resistant	Unauthorized Entry Pg. 16	$25,000
14SW-01-PACS: System, Physical Access Control	Unauthorized Entry	$30,000
	Total Funding Requested:	$70,000

INVESTMENT JUSTIFICATION (CONTINUED)

Drop downs will assist with section IV-B.

NONPROFIT SECURITY GRANT PROGRAM AUTHORIZED EQUIPMENT LIST

14CI-00-COOP	System, Information Technology Contingency Operations	Back-up computer hardware, operating systems, data storage, and application software necessary to provide a working environment for contingency operations. May be a purchased remote service or a dedicated alternate operating site.
14EX-00-BCAN	Receptacles, Trash, Blast-Resistant	Blast-resistant trash receptacles.
14EX-00-BSIR	Systems, Building, Blast/Shock/Impact Resistant	Systems to mitigate damage from blasts, shocks, or impacts, such as column and surface wraps, wall coverings, breakage/shatter resistant glass, window wraps, and deflection shields.
14SW-01-ALRM	Systems/Sensors, Alarm	Systems and standalone sensors designed to detect access violations or intrusions using sensors such as door/window switches, motion sensors, acoustic sensors, seismic, and thermal sensors. May also include temperature sensors for critical areas.
14SW-01-DOOR	Doors and Gates, Impact Resistant	Reinforced doors and gates with increased resistance to external impact for increased physical security.
14SW-01-EXTM	System, Fire Extinguisher Monitoring	System for monitoring the presence and pressure of fixed-location fire extinguishers to ensure that they are usable and are not stolen for possible misuse.
14SW-01-LITE	Lighting, Area, Fixed	Fixed high-intensity lighting systems for improved visibility in areas such as building perimeters and surveillance zones.
14SW-01-PACS	System, Physical Access Control	Locking devices and entry systems for control of physical access to facilities.
14SW-01-SIDP	Systems, Personnel Identification	Systems for positive identification of personnel as a prerequisite for entering restricted areas or accessing information systems.
14SW-01-SIDV	Systems, Vehicle Identification	Systems for identification of vehicles, ranging from decals to radio frequency identification (RFID) or other transponder devices.
14SW-01-SNSR	Sensors/Alarms, System and Infrastructure Monitoring, Standalone	Standalone sensors/alarms for use on critical systems or infrastructure items (security systems, power supplies, etc.) to provide warning when these systems fail or are near failure.
14SW-01-VIDA	Systems, Video Assessment, Security	Camera-based security systems utilizing standard, low light, or infrared technology.
14SW-01-WALL	Barriers: Fences; Jersey Walls	Obstacles designed to channel or halt pedestrian or vehicle-borne traffic in order to protect a physical asset or facility.
15IN-00-XRAY	System, Mobile Search & Inspection; X-Ray	Portable X-Ray systems for use in search and screening operations.
15SC-00-PPSS	Systems, Personnel/Package Screening	Hand-held or fixed systems such as walk-through magnetometers and conveyor-belt x-ray systems used to screen personnel and packages for hazardous materials/devices.

FINDING AUTHORIZED EQUIPMENT

- https://www.fema.gov/grants/tools/authorized-equipment-list

14SW-01-VIDA – Systems, Video Assessment, Security

Description:

Camera-based security systems utilizing standard, low light, or infrared technology.

This functionality may also be obtainable via subscription as a cloud-based service using a web browser interface or a mobile app, with imagery stored in the cloud as opposed to local software and storage. However, special security considerations apply for data stored remotely, including evidentiary issues for stored video. See 04AP-11-SAAS for further information.

Grant Notes:

Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities.

FEMA Related Grant Programs:

- Emergency Management Performance Grants (EMPG),Intercity Bus Security Grant Program (IBSGP)
- Operation Stonegarden (OPSG)
- Port Security Grant Program (PSGP)
- State Homeland Security Program (SHSP)
- Tribal Homeland Security Grant Program (THSGP)
- Transit Security Grant Program (TSGP)
- Urban Areas Security Initiative Program (UASI)
- Amtrak - (IPR - Amtrak)
- Environmental Planning and Historic Preservation (EHP)
- Homeland Security Grant Program (HSGP)
- Nonprofit Security Grant Program (NSGP)

ALLOWABLE COSTS

Equipment

Allowable costs are focused on target hardening and physical security enhancements. *Must align to the Authorized Equipment List in Section IV-B.*

Planning

Funding may be used for security or emergency planning expenses and the materials required to conduct planning activities.

Training

Allowable training topics are limited to the protection of critical infrastructure key resources, including physical and cybersecurity, target hardening, and terrorism awareness/employee preparedness such as Community Emergency Response Team training, Active Shooter training, and emergency first aid training. Proposed attendance at training courses and all associated costs using the NSGP must be included in the nonprofit organization's Investment Justification.

Exercise

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.

Hiring

Contracted Security Personnel are allowed under this program only as described in the NOFO and Manual. The NSGP funds may not be used to purchase equipment for contracted security. *The recipient must be able to sustain this capability in future years without NSGP funding.*

Management and Administration (M&A)

Management and Administration (M&A) activities are those costs defined as directly relating to the management and administration of NSGP funds, such as financial management and monitoring. *Must be requested at time of application. Cannot be added after award.*

INVESTMENT JUSTIFICATION (CONTINUED)

PART V. MILESTONE (5 POSSIBLE POINTS OUT OF 40)		
Provide descriptions and associated key activities that lead to the milestone event over the NSGP period of performance.		
Start dates should reflect the start of the associated key activities and end dates should reflect when the milestone event will occur. Milestones should reflect considerations to Environmental Planning and Historic Preservation reviews when applicable. *(10 milestones maximum)*		
KEY ACTIVITIES & CORRESPONDING MILESTONES	START DATE	COMPLETION DATE

MILESTONE EXAMPLES

Milestones are key actions towards project completion and provide a performance measure for monitoring project progress. Estimated completion dates must be included with each milestone in the Investment Justification. Listed below are examples of major activities, or milestones, and target completion dates.

1. Sign and return NSGP grant agreement documentation and attend the NSGP rollout meeting (November 2024);
2. Contact vendor(s) for updated price quotes (January 2025);
3. Complete and submit the eligibility forms (February 2025);
4. Complete and submit the Environmental and Historic Preservation (EHP) documentation (March 2025);
5. Purchase reinforced door, locks and wiring (April 2025);
6. Complete deconstruction of doorway (May 2025);
7. Install reinforced door with locks and wiring (June 2025);
8. Progress reports to state and local partners (July 2025);
9. Submit reimbursement documentation (August 2025).

INVESTMENT JUSTIFICATION (CONTINUED)

PART VI. PROJECT MANAGEMENT (2 POSSIBLE POINTS OUT OF 40)

Who will manage the project? *Include the name, phone number, email address, and experience of the project manager(s).*

Examples:
Project Manager Lead: Jack Ryan, 511-119-2323, JackRyan@gmail.com, CEO for 5 years at CIA School of Health and have been awarded and managed Department of Health grants for the past 3 years.

Project Manager Backup: Jim Greer, 232-111-1234, JimGreer@gmail.com, Financial Manager for 3 years at CIA School of Health and have experience managing Department of Health grants for the past 3 years.

Please assess your project management plan/approach. Assessment could include challenges to the effective implementation of this project and the coordination of the project with State and local homeland security partners.

Examples:
Challenges to effectively implement this project include installing the reinforced doors outside of the school year, preferably in the summer and learning how to manage a new grant while still managing our grant from Department of Health.

Coordination efforts for the project will include state partners such as Michigan State Police, Emergency Management and Homeland Security Division, Michigan Department of Education, and the Michigan Department of Health and Human Services. Local Agencies that our organization will coordinate with include Secret County Sheriff's Office, Secret Counties Educational Board, and Secret Counties Fire Department.

INVESTMENT JUSTIFICATION (CONTINUED)

PART VII. IMPACT (4 POSSIBLE POINTS OUT OF 40)

Please describe the measurable outputs and outcomes that will indicate that this Investment is successful at the end of the period of performance.

Example:
Once the reinforced doors are installed, we will conduct an active shooter exercise and test the doors automatic locking mechanism. The after-action report will include whether the doors were able to automatically lock from the panic buttons alarm before the active shooter was able to enter the building from the parking lot and whether the doors were able to be unlocked remotely from our control center.

Example:
This project supports the Access Control and Identity Verification core capability and reduces the applicable gaps of our facility that includes control and limit access to critical locations and systems to authorized individuals carrying out legitimate activities. A reinforced door will build on our effort to reduce our security gap of controlling and limiting access to our facility.

INVESTMENT JUSTIFICATION (CONTINUED)

FUNDING HISTORY
If the nonprofit organization has received NSGP funding in the past, provide the funding amount, funding year, and the investment type.
Has the organization received NSGP funding in the past?   Yes   No   ▼
If "Yes," please list the year(s), amount(s), and Project(s)/Investment(s). (Example: FY20 / $150K / CCD Camera System and Lighting.)

NONPROFIT SUBAPPLICANT CONTACT INFORMATION	
This application was written by: ▼	
☐ By clicking this box, I certify that I am an employee or affiliated volunteer on behalf of the nonprofit organization or have been hired by the nonprofit organization to apply on their behalf for the Nonprofit Security Grant Program.	
FULL NAME	POSITION/TITLE
EMAIL	WORK PHONE

VULNERABILITY ASSESSMENTS

A vulnerability/risk assessment specific to the location/facility for which the nonprofit organization is applying for funding is REQUIRED. Currently, there are no other requirements for the vulnerability assessment, but it must be thorough and specific to your organization.
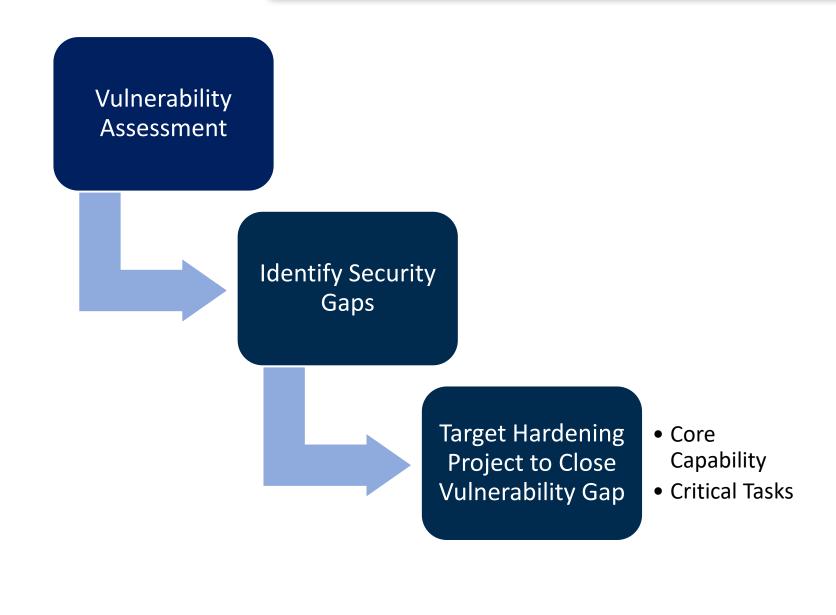
If you do not have a vulnerability assessment, get one now. Your project must link to identified vulnerabilities within your vulnerability assessment. You can pay for someone to complete a vulnerability assessment or at times your local police department may assist with this depending on staffing.

An example of a vulnerability may be that your organization's facility has a glass door that does not lock, and you would like to purchase a reinforced door. Your vulnerability assessment must identify the glass door as a vulnerability. Your project should describe activities you are requesting grant funds for to address the vulnerability, such as replacing the door with a reinforced door with an automatic locking mechanism to harden your facility.
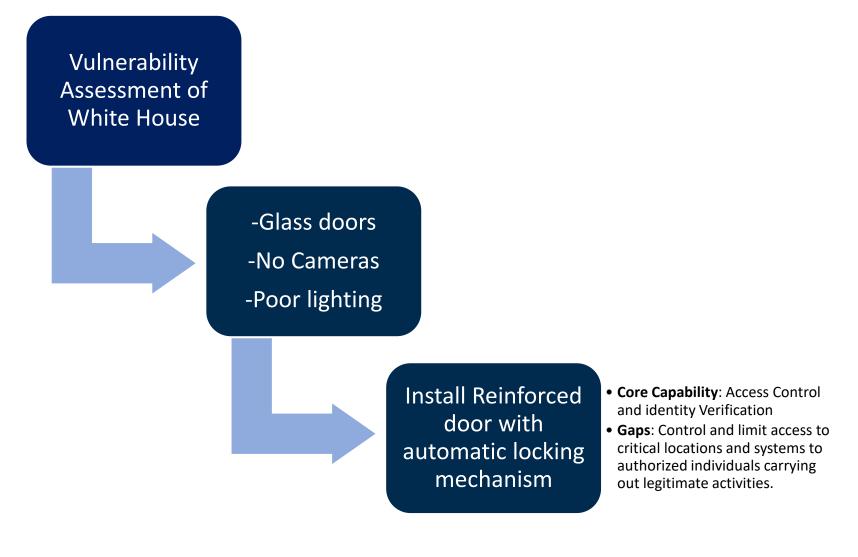
If your project is to purchase a reinforced door but your vulnerability assessment does not mention any need for a new reinforced door, then the door in your project would be unallowable.

WHAT MAKES A STRONG APPLICATION?

—

- **Clearly identified risks, vulnerabilities, and consequences.**

- **Description of findings from a previously conducted vulnerability assessment.**

- Details of any incident(s) including description, dates, etc.

- A brief description of any supporting documentation that is submitted as part of the application, if applicable.

- **Explanation of how the investments proposed will mitigate or address the vulnerabilities identified from a vulnerability assessment.**

- Establish a clear linkage with investment(s) and core capabilities.

- **Verify all proposed activities are allowable costs per the FY 2024 NSGP NOFO.**

- Realistic milestones that considers the EHP review process, if applicable.

- Description of the project manager(s) level of experience.

Example

Vulnerability Assessment of White House

-Glass doors

-No Cameras

-Poor lighting

Install Reinforced door with automatic locking mechanism

- **Core Capability**: Access Control and identity Verification
- **Gaps**: Control and limit access to critical locations and systems to authorized individuals carrying out legitimate activities.

What Critical Task does your target hardening activity support?

NONPROFIT SECURITY GRANT PROGRAM COMMON CORE CAPABILITIES

The National Preparedness Goal is published by FEMA and below are the common core capabilities used for the NSGP.

Protection – **Physical Protective Measures:** Implement and maintain risk-informed countermeasures, and policies protecting people, borders, structures, materials, products, and systems associated with key operational activities and critical infrastructure sectors.

- Reducing or mitigation risks, including actions targeted at threats, vulnerabilities, and/or consequences, by controlling movement and protecting borders, critical infrastructure, and the homeland.

Protection – **Access Control and Identity Verification:** Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.

- Implement and maintain protocols to verify identity and authorize, grant, or deny physical and cyber access to specific locations, information, and networks.

COMMON PITFALLS

- Failure to have a thorough vulnerability/risk assessment.
- Failure to answer the question being asked or only answering part of the question.
    - Hint: There is a difference between "and" and "or."
- Failure to establish a clear link between the proposed project and the identified vulnerabilities.
- Failure to submit the required supporting documentation.
    - Examples: Contact sheet, Mission Statement, Vulnerability Assessment.
    - The MSP/EMHSD will provide a list of the required documents after the release of the NOFO.
- Requesting unallowable equipment.
- Failure to submit before the deadline (This is a competitive process; and late submissions will not be accepted).

READ AND FOLLOW INSTRUCTIONS

The NSGP application is set up to ensure that individuals without grant application experience can complete the application successfully. It is very important to read each, and every set of instructions provided by either MSP/EMHSD or FEMA. If there is something you do not understand after reading the instructions, contact the MSP/EMHSD and we will happily assist you.

DO NOT FEED THE LION

Ever wish you'd read the instructions?

CONTACT INFORMATION SHEET

APPLICATION DOCUMENT #3

CONTACT INFO SHEET

Name of Organization: ▭

Organization Type:
  1) Ideology-based/Religious/Spiritual/Secular ____
  2) Medical ____
  3) Educational ____
  4) Other ____

Point of Contact: ▭

Contact Email: ▭

Address of the Nonprofit Organization: ▭

City: ▭

Zip Code: ▭

County: ▭

Telephone Number: ▭

CONTACT INFO SHEET CONTINUED

Telephone Number: [____]

If Application submitted by other than Point of Contact, please provide name, email and phone number of individual submitting: [____] [____] [____]

UEI(SAM.GOV): [____]

EIN: [____]

Congressional District: [____]

Elected Official: [____]

EXECUTIVE COMPENSATION
APPLICATION DOCUMENT #4

EXECUTIVE COMPENSATION

- Required by Code of Federal Regulations to submit the Federal Funding Accountability and Transparency Act (FFATA) sub-award reports.

- Applies to all federal funds.

If a subrecipient:

1. Receives 80% or more of annual revenues from federal funds; *AND,* $25 million or more in annual revenue from federal funds.

- If your organization meets the threshold, you are required to report the compensation of the five highest paid executives in your organization.

- The MSP/EMHSD is collecting executive compensation data from applicants during the application process. Applications will be submitted using "SmartSheet" and will include questions relating to executive compensation.

- The FFATA reports are available on USASpending.gov.

- If your organization has an active sam.gov account and meets the threshold, your organization is likely already reporting this information.

MISSION STATEMENT

Quote is from FEMA – NOFO.

 Mission Statement

"Each nonprofit subapplicant must include its Mission Statement and any mission implementation policies or practices that may elevate the organization's risk. SAAs will use the Mission Statement along with the nonprofit subapplicant's self-identification in the IJ to validate that the organization is one of the following types: 1) Ideology-based/Spiritual/Religious; 2) Educational; 3) Medical; or 4) Other. The organization type is a factor when calculating the final score of the application…"

APPLICATION PACKET RECAP

A complete application packet must include:

- Nonprofit Security Grant Program (NSGP) Investment Justification (Application);
- Executive Compensation;
- Contact Info Sheet;
- Vulnerability Assessment;
- Mission Statement.

Do not try to submit documents on grants.gov.
- **Applications must be submitted through a portal called "Smartsheet."**
    - **You will receive a message, "Success! We've received your information."**
    - **If you would like a copy of your submission, be sure to check the box on the form.**

SCORING CRITERIA OVERVIEW

SCORING CRITERIA

The applications are scored in groups based on location in the State. The NSGP-S applications are reviewed by a state review committee. The NSGP-UA applications are scored by an Urban Areas Security Initiative (UASI) review committee, which is made up of emergency managers or their designee from the counties in the UASI region.

Once scoring and prioritization occurs at the state level the applications are submitted to FEMA, where a second scoring process is conducted at the federal level. **The FEMA makes the actual determination of who receives funding**.

All completed applications are submitted for federal review; however, we do **NOT** submit applications that are incomplete. Ensure that you complete each box on your application.

SCORING CRITERIA

Nonprofit Security Grant Program Scoring Matrix – Fiscal Year 2023

Reviewers should use this document as a reference when scoring applications under the Fiscal Year (FY) 2023 Nonprofit Security Grant Program (NSGP).

I – Applicant Information			
Question	**Criteria**	**Score**	**Explanations**
1 Did the applicant provide all the required information in the Applicant Information Section?	The applicant should provide all information as it is applicable in the informational section.	Yes	The applicant **did** provide all the required information.
		No	The applicant **did not** provide all the required information.

II - Background			
Question	**Criteria**	**Score**	**Explanations**
2 Did the applicant provide a description of their nonprofit organization to include symbolic value of the site as a highly recognized national or historical institution or as a significant institution within the community that renders the site as a possible target of terrorism and other extremist attacks?	Applicants must describe their organization, its mission/purpose, the symbolic value of the building/organization, and how these factors may make it the target of an attack.	0	The applicant **did not provide a description** of the organization including the symbolic value of the site as a highly recognized institution that renders the site a possible target of terrorism or other extremist attacks.
		1	The applicant **provided a poor description** of the organization including the symbolic value of the site as a highly recognized institution that renders the site a possible target of terrorism or other extremist attacks.
		2	The applicant **provided an adequate description** of the organization including the symbolic value of the site as a highly recognized institution that renders the site a possible target of terrorism or other extremist attacks.
		3	The applicant **provided a full, clear, and effective description** of the organization including the symbolic value of the site as a highly recognized institution that renders the site a possible target of terrorism or other extremist attacks.
3 Did the applicant provide a description of their nonprofit organization to include any role in responding to or recovering from events that integrate nonprofit preparedness with broader state/local preparedness efforts?	Applicants must clearly describe their individual organization's previous or existing role in response to or in recovery efforts to terrorist or other extremist attacks. This should tie into the broader preparedness efforts of state and/or local government.	0	The applicant **did not provide a description** of the organization that included any role in responding to or recovering from events that integrate nonprofit preparedness with broader state/local efforts.
		1	The applicant **provided some description** of the organization that included any role in responding to or recovering from events that integrate nonprofit preparedness with broader state/local efforts.
		2	The applicant **provided a full, clear, and effective description** of the organization that included any role in responding to or recovering from events that integrate nonprofit preparedness with broader state/local efforts.

SCORING CRITERIA

III - Risk			
Question	**Criteria**	**Score**	**Explanations**
4 Did the applicant discuss specific threats or attacks against the nonprofit organization or closely related organization?	To substantiate the applicant's risk to a terrorist or other extremist attack, applicants may describe incidents that have occurred at or threats that have been made to their organization. Applicants may also draw from incidents that have occurred at closely related/similar organizations either domestically or internationally; the applicant should make the connection that they are at risk for the same reasons. Local crimes such as burglary, theft, or vandalism without a terrorism, extremism, or hate-related nexus may provide context justification for NSGP funding.	0	The applicant **did not discuss specific** threats or attacks against the organization or a closely related organization.
		1	The applicant **provided minimal discussion** of threats or attacks against the organization or a closely related organization.
		2	The applicant **provided poor discussion** of threats or attacks against the organization or a closely related organization.
		3	The applicant **provided adequate discussion** of threats or attacks against the organization or a closely related organization.
		4	The applicant **provided good discussion** of threats or attacks against the organization or a closely related organization.
		5	The applicant **provided multiple, detailed, and specific** threats or attacks against the organization or a closely related organization.
5 In considering vulnerabilities, how well did the applicant describe the organization's susceptibility to destruction, incapacitation, or exploitation by a terrorist or other extremist attack?	Applicants must provide a clear description of findings from a completed vulnerability assessment.	0	The applicant **did not discuss or describe** the organization's susceptibility to attack.
		1	The applicant **provided minimal description** of the organization's susceptibility to attack.
		2	The applicant **provided poor description** of the organization's susceptibility to attack.
		3	The applicant **provided adequate description** of the organization's susceptibility to attack.
		4	The applicant **provided good description** of the organization's susceptibility to attack.
		5	The applicant **provided clear, relevant, and compelling description** of the organization's susceptibility.
6 In considering potential consequences, how well did the applicant address potential negative effects on the organization's asset, system, and/or network if damaged, destroyed, or disrupted by a terrorist or other extremist attack?	Applicants should describe how an attack would impact them, the community served, and if possible/applicable, beyond the immediate individuals served (nearby critical infrastructure, businesses, transportation, schools, etc.).	0	The applicant **did not discuss or describe** the potential negative consequences the organization may face.
		1	The applicant **provided minimal description** of the potential negative consequences the organization may face.
		2	The applicant **provided poor description** of the potential negative consequences the organization may face.
		3	The applicant **provided adequate description** of the potential negative consequences the organization may face.
		4	The applicant **provided good description** of the potential negative consequences the organization may face.
		5	The applicant **provided a clear, relevant, and compelling description** of the potential negative consequences the organization may face.

SCORING CRITERIA

IV – Facility Hardening				
Question		**Criteria**	**Score**	**Explanations**
7	How well does the applicant describe the proposed facility hardening activities, projects, and/or equipment and relate their proposals to the vulnerabilities described in Question 6?	In narrative form in Section IV-A, applicants must clearly explain what the proposed activities, projects, and/or equipment are, identify their estimated cost, and describe how they will mitigate or address vulnerabilities identified in the vulnerability assessment in Section III (Question 6).	0	The applicant **did not propose** facility hardening or the proposals do not mitigate identified risk(s) and/or vulnerabilities.
			1	Proposed activities, projects, or equipment **may provide minimal** facility hardening **or are only minimally related** to some of the identified risk(s) and/or vulnerabilities.
			2	Proposed facility hardening activities, projects, or equipment **would likely mitigate** identified risk(s) and/or vulnerabilities.
			3	Proposed facility hardening activities, projects, or equipment are **clearly aligned with and effectively mitigate** the identified risk(s) and/or vulnerabilities.
8	Did the applicant's proposed facility hardening activity focus on the prevention of and/or protection against the risk of a terrorist or other extremist attack?	The proposed activities, projects, and equipment should directly tie to the prevention of and/or protection against the risk of terrorist or other extremist attacks.	0	The proposed facility hardening activities **do not focus** on the prevention of and/or protection against the risk of terrorist or other extremist attacks.
			1	The proposed facility hardening activities **are somewhat focused** on the prevention of and/or protection against the risk of terrorist or other extremist attacks.
			2	The proposed facility hardening activities **are adequately focused** on the prevention of and/or protection against the risk of terrorist or other extremist attacks.
			3	The proposed facility hardening activities **are clearly and effectively focused** on the prevention of and/or protection against the risk of terrorist or other extremist attacks.
9	Are all proposed equipment, activities, and/or projects tied to a vulnerability that it could reasonably address/mitigate?	The proposed equipment, activities, and/or projects should mitigate/address the vulnerability tied to it in the Section IV-B table.	0	**No vulnerabilities are listed** and/or the proposed equipment, activities, or projects **do not address listed vulnerabilities.**
			1	The proposed equipment/activities/projects **are somewhat reasonable** to address the listed vulnerability.
			2	The proposed equipment/activities/projects **are mostly reasonable to address** the listed vulnerability.
			3	The proposed equipment/activities/projects **effectively address** the listed vulnerability.

SCORING CRITERIA

V - Milestones			
Question	**Criteria**	**Score**	**Explanations**
10 How well did the applicant describe the milestones and the associated key activities that lead to the milestone event over the NSGP period of performance?	The applicant should describe the milestones needed to accomplish the goals of the NSGP funding and should include the key activities that will be necessary to accomplish those milestones.	0	The applicant **did not provide** information on milestones and associated key activities.
		1	The applicant **provided some description** of milestone events and the associated key activities over the NSGP POP.
		2	The applicant **provided adequate description** of milestone events and the associated key activities over the NSGP POP.
		3	The applicant **fully and effectively described** milestone events and the associated key activities over the NSGP POP.
11 Did the applicant include milestones and associated key activities that are feasible over the NSGP period of performance?	Milestones should be realistic, potentially include the entire period of performance (36 mo.), be inclusive of all proposed activities, and consider the Environmental Planning and Historic Preservation review process. Milestones should not exceed 36 months and should not begin prior to the Period of Performance.	0	The applicant **did not include** milestones and key activities that are feasible over the NSGP POP.
		1	The applicant included milestones and key activities that are **somewhat feasible** over the NSGP POP.
		2	The applicant included milestones and key activities that **are feasible** over the NSGP POP.
VI – Project Management			
Question	**Criteria**	**Score**	**Explanations**
12 How well did the applicant justify the effectiveness of the proposed management team's roles and responsibilities and the governance structure to support implementation of the Investment?	Brief description of the project manager(s) and level of experience.	0	The applicant **did not justify** the effectiveness of proposed management team or the structure in place to support implementation.
		1	The applicant **somewhat justified** the effectiveness of the proposed management team and the structure in place to the support implementation.
		2	The applicant **fully justified** the effectiveness of the proposed management team and the structure in place to the support implementation.

SCORING CRITERIA

VII – Impact				
Question		**Criteria**	**Score**	**Explanations**
13	How well did the applicant describe the outcomes/outputs that would indicate that the Investment was successful?	Measurable outputs and outcomes should directly link to the vulnerabilities and consequences outlined in Section III.	0	The applicant **did not describe** the outcomes and/or outputs that would indicate the Investment was successful.
			1	The applicant **provided minimal information** on the outcomes and/or outputs that would indicate the Investment was successful.
			2	The applicant **provided some information** on the outcomes and/or outputs that would indicate the Investment was successful.
			3	The applicant **provided an adequate discussion** of the outcomes and/or outputs that would indicate the Investment was successful.
			4	The applicant **provided a full and detailed description** of the outcomes and/or outputs that would indicate the Investment was successful.

PROJECT CHANGES

The NSGP is competitive, and funding decisions are based on:

- The threat, vulnerability, and consequence to a specific facility/location.

- The ability of the proposed project to mitigate the risk factors identified in the investment and risk assessment.

Due to the competitive nature of the grant, the Department of Homeland Security and FEMA will generally not approve scope changes resulting from the following situations: Requests to fund projects at alternative facilities.

- Circumstances where renovations are completed after the application is submitted that impact vulnerabilities upon which the application was developed.

- Requests to significantly change the physical security enhancements for which funding was originally provided.

WHAT TO EXPECT IF AWARDED/ KEY POINTS

- You will receive the award notification email. No money can be spent at this time. Last year notifications went out in August.

- This grant is *reimbursement* based. The subrecipient will pay for the project and be reimbursed for the allowable work completed.

- Multiple steps once awarded- Grant Agreements, Alignment and Allowability forms, Procurement process, EHP form approvals, work on project, reimbursement packets, and Biannual Strategy Implementation Report/Closeout.

- It can be difficult to change the scope of work once awarded. Please keep this in mind when working on Section IV-B of the investment justification. These categories will be what you will be awarded on.

- Lots of documentation will be involved with the award. A webinar will be hosted for each step along the way.

IMPORTANT POINTS

- Program is designed for enhancing physical security measures in existing structures.

- Applications MUST be submitted through our website.

- Risk/vulnerability assessments.

- The application is a PDF format.

- UEI → It may take a while for this process, please ensure this is done in a timely manner.

- 501(c)(3) number → use EIN.

- Read the NOFO and FEMA Grants Preparedness Manual NSGP appendix.

- ***Proofread.***

- *** It is very important to read directions and follow instructions. ***

QUESTIONS?

CONTACT INFORMATION

NSGP - PRIMARY CONTACT:

Jason Guthaus

Phone: 517-614-0936

Email: GuthausJ1@michigan.gov

NSGP - BACK UP CONTACT:

Paul Lounsberry

Phone: 517-256-3920

Email: LounsberryP@michigan.gov