

NONPROFIT SECURITY
GRANT PROGRAM –
NATIONAL SECURITY
SUPPLEMENTAL (NSGP-NSS)



Introductions

Topics of Discussion

- What is it?
- Grant Funding
- Who can apply
- What's Eligible
- Timeline
- Application Process, Documents, and Due Dates
- Requirements if Awarded
- Q&A

AGENDA

WHAT IS IT?

The Nonprofit Security Grant Program – National Security Supplemental will improve and increase the physical/cyber security and facility/target hardening of nonprofit organizations' facilities at risk of a terrorist or other extremist attack, ultimately safeguarding the lives and property of the American people.

All NSGP-NSS activities must be linked to enhancing the security and safety at the physical site of the nonprofit organization. Concurrently, the NSGP-NSS will integrate the preparedness activities of nonprofit organizations that are at risk of a terrorist or other extremist attack with broader state and local preparedness efforts.

The NSGP-NSS supplements one of three grant programs that support DHS/FEMA's focus on enhancing the ability of state, local, tribal, and territorial governments, as well as nonprofits, to prevent, protect against, prepare for, and respond to terrorist or other extremist attacks.

WHAT IS IT?

\$210 million in additional funds are a portion of the \$390 million that were included in the fiscal year 2024 National Security Supplemental, a key priority of the Biden-Harris Administration as it continues to intensify its efforts to combat the dramatic increase in hate crimes and other forms of targeted violence against faith-based institutions and nonprofit organizations.

The first tranche was made available in June 2024. In total for fiscal year 2024, the Administration has secured \$664 million for the NSGP, more than double last year's \$305 million appropriation.

Eligible subapplicants for this program must meet the definition of nonprofit organization described under section 501(c)(3) of the Internal Revenue Code of 1986 (IRC) and exempt from tax under section 501(a) of such code;

AND: Be able to demonstrate, through application, that the organization is at high risk of a terrorist or other extremist attack;

AND: Be located outside of a UASI- designated urban area (all nonprofits physically in Alaska meet this requirement);

AND: The organization must agree to comply with the standards, regulations, and requirements applicable to subrecipients receiving pass-through subawards found in 2 CFR Part 200—Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards

The State of Alaska WILL NOT be accepting Consortium Applications in the FY24 NSGP-NSS

WHO'S ELIGIBLE?

Target allocation for FY 2024 NSGP-NSS is \$1,567,200

Alaska's FY2024 NSGP funding: \$2,094,756

GRANT FUNDING

NSGP Overview: Eligibility

What type of entities/organizations are eligible to apply under NSGP?

The list below is not exhaustive and only provides examples of potential eligible organizations, all of which must be nonprofits.

- | | |
|--|---|
|  Houses of worship |  Shelters/crisis centers |
|  Educational facilities |  Event venues |
|  Medical facilities |  Science organizations |
|  Senior centers/care facilities |  Camps |
|  Community/social service |  Museums |

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.

What type of entities/organizations are not eligible to apply under NSGP?

- | | |
|--|---|
|  Utility companies |  Organizations active in politics/lobbying |
|  Governmental entities |  For-profit venues, stadiums, amusement parks, etc. |
|  For-profit hospitals |  Homeowner associations, labor unions, etc. |
|  For-profit colleges/universities |  For-profit transportation entities |
|  Volunteer fire departments |  Municipal/public schools (elementary, middle, high) |
|  Kiwanis, Rotary, Lions Clubs, etc. | |

WHO'S ELIGIBLE?

- ▶ Nonprofit organizations must have a Unique Entity Identifier (UEI), which is obtained through [SAM.gov](https://sam.gov).
- ▶ *Nonprofit organizations are not required to have a UEI issued at the time of application* but **MUST** have a valid UEI to receive a subaward from the SAA.
- ▶ Nonprofit organizations must register in SAM.gov to obtain the UEI **but are not required to maintain an active registration in SAM.gov**. Guidance on obtaining a UEI in SAM.gov can be found at [GSA UEI Update](#) and the [Federal Service Desk Knowledge Base](#).
- ▶ It may take four weeks to obtain a UEI, and applicants should plan accordingly. **Obtaining a UEI does not cost anything; it is free of charge.**

WHO'S ELIGIBLE?

WHAT'S ELIGIBLE?

Each subapplicant may apply for up to \$200,000 in the form of an Investment Justification (IJ). The IJ must describe each investment proposed for funding and all of the below:

- ▶ Be for the location(s)/physical address(es) (NOT P.O. Boxes) that the nonprofit occupies at the time of application;
- ▶ Address an identified risk, including threat and vulnerability, and build or sustain a core capability identified in the National Preparedness Goal
- ▶ Demonstrate the ability to provide enhancements consistent with the purpose of the program and guidance provided by DHS/FEMA
- ▶ Be both feasible and effective at reducing the risks for which the project was designed
- ▶ Be able to be fully completed within the two-year period of performance

Note:

No more than 2 locations per Non-Profit!

Each location must be a separate IJ!

Security Related Projects:

Planning: Must be related to the protection of the facility and the people within.

Training: Security related training for security personnel and for nonprofit employees, members, congregants, and volunteers,
no travel costs

Contracted security personnel

Exercises: Plan and conduct security-related exercises.

Equipment: Facility hardening and physical security enhancements.

WHAT'S ELIGIBLE? (CONT.)

NSGP Overview: Allowable vs. Unallowable Expenditures

✓ Allowable Examples

- ✓ Access controls / Cybersecurity
- ✓ Bollards, barriers, and fences
- ✓ Blast-resistant doors, windows, etc.
- ✓ Contract security
- ✓ CCTV/Security Cameras
- ✓ Management & Administration (M&A)



FEMA

✗ Unallowable Examples

- ✗ License plate reader software
- ✗ Weapons and/or weapons training
- ✗ Facial recognition software
- ✗ General expenses, salaries, OT
- ✗ Knox boxes/key safe
- ✗ Proof-of-concept initiatives/studies

Federal Emergency Management Agency

11

ALLOWABLE VS. UNALLOWABLE



The FFY 2024 Federal Notice of Funding Opportunity (NOFO) released - Nov 25th



Applications for review and feedback due to mva.grants@alaska.gov by December 13th



Completed Application due to mva.grants@alaska.gov on December 23rd, 12:00pm



State submits federal application by January 24th



State receives federal award by May 10th



Projected Period of Performance 6/1/25 – 4/30/27

FFY 2024 NSGP-NSS PROJECTED TIMELINE

APPLICATION - PROCESS

1. FEMA Releases Notice of Funding Opportunity and Investment Justification Form with the application deadline for the State **(NOT the nonprofit)**.
2. DHS&EM will create its overview and guidelines with additional information and requirements.
3. DHS&EM sends out an email notification that the application is open and that non-profits have a different/earlier deadline to submit.
4. Applications must be submitted to DHS&EM at mva.grants@alaska.gov
5. DHS&EM reviews, scores and prioritizes applications for submittal to FEMA by application deadline.
6. FEMA reviews and determines project funding.

APPLICATION – VULNERABILITY ASSESSMENT

The Vulnerability Assessment is different from a risk/threat assessment. A risk assessment involves looking outside of an organization to determine external threats that exist that could potentially lead to security issues, whereas a vulnerability assessment involves looking inside the organization for internal vulnerabilities and weaknesses.

A vulnerability assessment is used to identify and validate physical security deficiencies of your organization/facility and is the foundation of an NSGP-NSS application.

Vulnerability assessments can be provided in the form of a Cybersecurity and Infrastructure Security Agency (CISA) Self-Assessment ([Facility Security Self-Assessment | CISA](#)), a state or local law enforcement assessment, an outside contractor's assessment, or other valid method of assessment.

APPLICATION – VULNERABILITY ASSESSMENT

Tom Koloski

Protective Security Advisor, State of Alaska

Cybersecurity and Infrastructure Security
Agency (CISA)

Cell: (907) 854-2417

Email: thomas.koloski@cisa.dhs.gov

APPLICATION – VULNERABILITY ASSESSMENT

Projects/activities requested through the NSGP-NSS should align to mitigate items identified in the Vulnerability Assessment. Vulnerability assessments are typically valid for as long as the items included in the assessment remain unaddressed/vulnerable.

FEMA recommends updating these assessments anytime there is a significant renovation, change, or resolution to a vulnerability, OR every five years. FEMA does not currently impose specific requirements on vulnerability assessments.

APPLICATION - DOCUMENTS

1. Investment Justification Application Form
2. Vulnerability Assessment/Risk Assessment specific to the facility being applied for.
3. Mission Statement - Each subapplicant must include its Mission Statement and any mission implementing policies or practices that may elevate the organization's risk. SAAs will use the Mission Statement along with information provided in the subapplicant's IJ in order to validate the organization is one of the following types: 1) Ideology-based/Spiritual/Religious (Houses of Worship, Religious Schools, etc.); 2) Educational (Secular), 3) Medical (Secular), or 4) Other
4. Signatory Authority Form with required three (3) signatures for organization.
5. If applicable, any Memorandum of Understanding (MOU), or Memorandum of Agreement (MOA) related to inter-agency projects.

APPLICATION



The application period for the 2024 NSGP-NSS is currently open. Applications are due Monday, December 23rd, 2024 at 12:00 PM AKST. The Investment Justification may appear as if it's not pulling up. Please click the link to the IJ and click download, save it to your computer, then open in Adobe.

Document Name	Document Type	Publish Date
2024 State Overview and Guidelines	PDF	November 2024
2024 Investment Justification	PDF	November 2024
Signatory Authority Form	PDF	November 2024
2024 FEMA NSGP-NSS NOFO	PDF	November 2024
2024 FEMA NSGP Preparedness Grants Manual	PDF	November 2024
2024 NSGP-NSS Authorized Equipment List	PDF	November 2024

When you click on the IJ link on our website it will open a new tab and appear like the below image. You will need to click on the save icon.

1 / 1 | - 100% + |

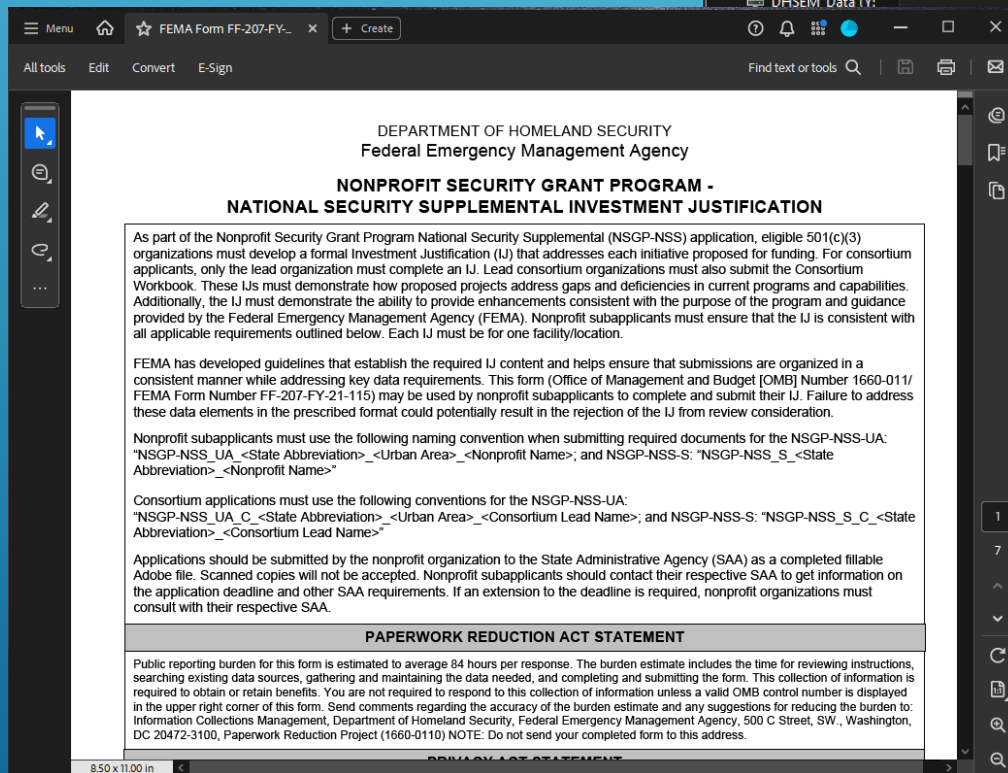
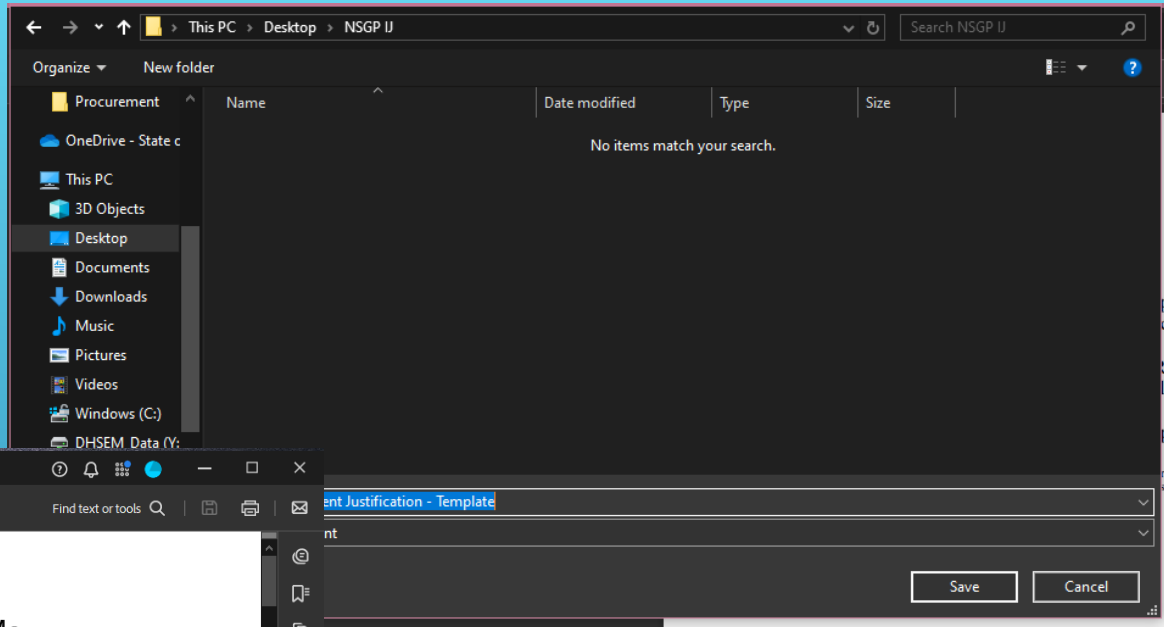


The document you are trying to load requires Adobe Reader 8 or higher. You may not have the Adobe Reader installed or your viewing environment may not be properly configured to use Adobe Reader.

For information on how to install Adobe Reader and configure your viewing environment please see http://www.adobe.com/go/pdf_forms_configure.

APPLICATION – INVESTMENT JUSTIFICATION

Save the IJ on your computer. Then once you open the IJ from that saved location it will appear like the below image.



The IJ will not open correctly in a web browser and must be opened from your computer in Adobe.

APPLICATION – IJ (CONT.)

PART I. NONPROFIT ORGANIZATION SUBAPPLICANT INFORMATION

Identify the following:

LEGAL NAME OF THE ORGANIZATION

Please list the physical address of the facility.

STREET

One investment justification per facility or per consortium application.

CITY

STATE

ZIP CODE

COUNTY

APPLICATION – IJ ORGANIZATION

Is this IJ submitted by the lead organization of a consortium? <input type="checkbox"/> Yes <input type="checkbox"/> No	
Note: Please answer Part II through Part VII of this IJ with summary responses that represent the collective of the consortium project(s). Additional space will be provided for further elaboration and narrative justification in the Consortium Workbook.	
Is the building owned, or are you leasing/renting? <input type="checkbox"/> Yes <input type="checkbox"/> No	If leasing or renting, do you have the owner's permission to make the proposed security enhancements? <input type="checkbox"/> Yes <input type="checkbox"/> No
At the time of application, is the organization actively occupying and functioning out of the location listed above? <input type="checkbox"/> Yes <input type="checkbox"/> No	
Are you the only nonprofit operating in/from this facility/building? <input type="checkbox"/> Yes <input type="checkbox"/> No	
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.	
If "No," please explain how the proposed security enhancements benefit both you and the other organization(s).	
<div style="background-color: #e0e0e0; height: 100px;"></div>	
Based on your mission statement, please summarize your organization's mission, ideology, and/or beliefs.	
<div style="background-color: #e0e0e0; height: 100px;"></div>	
What is the primary organization type?	<input type="checkbox"/> Ideology-based/Spiritual/Religious (Houses of Worship, Religious Schools, etc.) <input type="checkbox"/> Educational (Secular) <input type="checkbox"/> Medical (Secular) <input type="checkbox"/> Other
If "Other," please describe the type of org	<div style="background-color: #e0e0e0; height: 20px;"></div>

Best Practices

- ▶ Answer all required questions
- ▶ Describe but be concise

Common Pitfalls

- ▶ Being vague or assuming reviewer knows
- ▶ Not answering

APPLICATION – IJ ORGANIZATION (CONT.)

Please select the function that best describes the organization:

Please select the organization's primary affiliation:

Note: Please select the main religious affiliation that describes your organization. If the organization is a denomination of an affiliation, please select the corresponding affiliation from the drop down menu instead of "Other." If your organization has NO religious affiliation, please select "None/Unaffiliated." There is NO scoring preference given to certain affiliations or lack thereof.

If "Other," please describe affiliation.

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:

Nonprofits do not need to have a valid UEI at the time of application; however, subrecipients must have a valid UEI in order to receive a subaward.

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):

FEMA Form FF-207-FY-21-115 (formerly 089-25) (4/24) Page 2 of 7

House of Worship

Community Center

Pre-School

Elementary School

Middle School

High School

Post-Secondary Education

Other Type of Educational Organization

Social Services

Jewish

Christian

Hindu

Islamic

Sikh

Buddhist

Unaffiliated/None

Other

APPLICATION – IJ ORGANIZATION (CONT.)

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 or other extremist attack.

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.

prevention, protection, response, and/or recovery:



- Terrorist attack
- Man-made disaster (non-terrorist)
- Natural disasters
- Other

APPLICATION – IJ BACKGROUND

Best Practices

- ▶ Answer each separately
- ▶ Be concise
- ▶ Should be crafted using the identified threats/risks to your organization, the results of the Vulnerability Assessment of a physical location/structure/building, and details of the requested projects/activities to mitigate or remediate those vulnerabilities with associated estimated costs. Nonprofit organizations should describe their current threat/risk. While historic risk may be included context, the IJ should focus on current threats and risks.

Common Pitfalls

- ▶ Being vague or assuming the reviewer knows
- ▶ Not answering
- ▶ Answers should not be the same

PART III. RISK (15 POSSIBLE POINTS OUT OF 40)	
Is your organization facing heightened threat resulting from the Israel-Hamas war? <input type="checkbox"/> Yes <input type="checkbox"/> No	
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. <i>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.</i>	
<div style="background-color: #e6f2ff; height: 150px;"></div>	
B) Vulnerabilities: Please describe the organization's susceptibility to destruction, incapacitation, or exploitation by a terrorist or other extremist attack.	
<div style="background-color: #e6f2ff; height: 150px;"></div>	

APPLICATION – IJ RISK

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 or other extremist attack.



APPLICATION – IJ RISK (CONT.)

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.

Note: This section should include narrative information about all costs listed in Section IV-B. The objective is for the information contained in this section to allow reviewers to validate the need of all costs in Section IV-B.

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 or other extremist attack.

Best Practices

- ▶ Describe each project separately
- ▶ Address each aspect for each project
- ▶ Be concise!

Common Pitfalls

- ▶ Being vague or assuming the reviewer knows
- ▶ Not answering

APPLICATION – IJ FACILITY HARDENING

Nonprofit organizations should think broadly and holistically in their approach to security measures designed to protect buildings and safeguard people.

Some physical security control examples include locks, gates, and guards (e.g., contract security).

Although these may be effective measures, there are many additional layers to physical security that can help protect the organization, including creating comprehensive physical security plans, conducting training and exercises (e.g., active shooter, evacuation), identifying countermeasures against intrusion (e.g., access controls), preventing physical security breaches (e.g., security enhanced doors/windows), and monitoring for physical security threats (e.g., cameras, surveillance).

APPLICATION – IJ FACILITY HARDENING

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).*

Empty response area for project manager information.

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.

Empty response area for project management plan assessment.

APPLICATION – IJ PROJECT MANAGEMENT

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.

Best Practices

- ▶ Cover all aspects/projects
- ▶ Be concise!

Common Pitfalls

- ▶ Being vague or assuming reviewer knows
- ▶ Not answering

APPLICATION – IJ IMPACT

▶ Contact should be the person who has the authority for the non-profit and knowledge to answer any questions we may have.

▶ Other considerations: Be realistic, costs are increasing regularly. Your non-profit may want to look at taking a phased approach. Apply for the most important/impactful first.

APPLICATION – IJ CONTACT AND OTHER CONSIDERATIONS

NONPROFIT SUBAPPLICANT CONTACT INFORMATION	
This application was written by: <input type="text"/>	
<input type="checkbox"/> 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 National Security Supplemental.	
FULL NAME	POSITION/TITLE
<input type="text"/>	<input type="text"/>
EMAIL	WORK PHONE
<input type="text"/>	<input type="text"/>

Application **Review** Deadline

December 13, 2024 at 11:59 pm

(This is only if you'd like us to review and provide feedback on your application)

Environmental & Historic Preservation (EHP) Compliance

Build American Buy America Act (BABAA)

Quarterly Reporting

Procurement Requirements and Documentation

Monitoring

Inventory Reporting

See *2024 State Overview and Guidelines* for a full list of compliance requirements, available at: <https://ready.alaska.gov/Grants/NSGPS>

KEY REQUIREMENTS IF AWARDED

Application Elements Detailed

Reviewed by SAA ONLY

Materials required and/or requested by the SAA to validate the information in the IJ. The materials are not provided to FEMA reviewers and are not part of the federal scoring process.



Mission Statement: Used to validate information in the IJ and to categorize the facility (ideology-based, education, medical, and other). Consortium must submit mission statements for all organizations.



Completed Vulnerability Assessment: Identify vulnerabilities in context of the threats and consequences of potential events at a facility/site. Proposed equipment, projects, and activities should directly link to mitigating specific vulnerabilities included in the assessment. Provides the foundation of the IJ content. Contact your SAA for local requirements. Refer to the links provided by CISA on the resource slide for self-assessments or assistance. Consortium may develop shared or individual vulnerability assessments.



Supporting Documentation, if applicable: Materials to help validate/support or describe the threats, risks and vulnerabilities nonprofits may face, summarized within the investment justification, such as police or insurance reports. *Reach out to your SAA to better understand any state level requirements, processes, templates, timelines, etc.*

Reviewed by SAA and FEMA

The IJ and the Consortium Workbook (if applicable) are the only documents reviewed by FEMA.



Completed Investment Justification (IJ): Outlines the investment and relevant projects. Includes summaries of information provided in mission statements, VAs, etc. Requires a budget narrative and breakdown, timeline, and project plan.



Consortium Workbook: For consortia applications only. Will supplement the information provided in the lead organization's IJ.



FEMA

Federal Emergency Management Agency

APPLICATION – REVIEW

Bonus Points and Multipliers

Bonus Points

- Nonprofit organizations that have not previously received NSGP funding will not have bonus points added to their final score.
- Communities deemed disadvantaged by the Climate and Economic Justice Screening Tool (CEJST) will still be given 10 bonus points.
- The self-identified characteristics of the consortium lead only will be applied to determine Bonus Points and Multipliers.

New Multiplier

- Subapplicant's SAA score will be multiplied by a factor of four for nonprofit organizations facing heightened threat resulting from the Israel-Hamas war.
- Subapplicants must **draw a clear connection** between the heightened threat they face and the Israel-Hamas war in their project narratives to qualify for this multiplier.
- All other multipliers will remain the same.



Federal Emergency Management Agency

Applications are due

Monday, December 23rd by 12:00 pm

ready.alaska.gov/grants

1-800-478-2337 or 907-428-7000

Email: mva.grants@alaska.gov