



Nonprofit Security Grant Program

Washington State Program Overview

Chris Burd
NSGP Program Manager



Topics

- NSGP Objective & Eligibility
- Preparing to Apply & Application Components
- Application Scoring & Review Overview
- Application Timeline



What is the Nonprofit Security Grant Program?

The Nonprofit Security Grant Program (NSGP) is a U.S. Department of Homeland Security (DHS) preparedness grant program.

NSGP provides funding for physical and cybersecurity enhancements and other security-related activities to (eligible) **nonprofit organizations that are at high risk of a terrorist or other extremist attack**. The NSGP also seeks to integrate the preparedness activities of nonprofit organizations with broader state and local preparedness efforts.

All NSGP activities must be linked to enhancing the security and safety at the physical site of the nonprofit organization.



Nonprofit Security Grant Program (NSGP)

Who is it for?	What does it do?	What project types can NSGP funding be used for?
Awarded annually to eligible <u>nonprofits</u> with an overall grant performance period of 36 months.*	Provides funding support for security-related and physical security enhancements to nonprofit organizations that are at risk of terrorism or domestic violent extremism.	Facility target hardening, contracted security personnel, security training, security planning and security exercises, and limited cybersecurity.
*All selected NSGP applications will receive a standard 36-month agreement from the Washington Military Department.		



NSGP Eligibility Requirements

1. Eligible nonprofit organizations are those organizations that are 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

2. Ability to demonstrate, through the application, that the organization is at HIGH RISK of a terrorist attack or other extremist attack.

**Note: The Internal Revenue Service (IRS) does not require certain organizations such as churches, mosques, and synagogues to apply for and receive a recognition of exemption under section 501(c)(3) of the IRC. Such organizations are automatically exempt if they meet the requirements of section 501(c)(3). These organizations are not required to provide recognition of exemption.*

Examples of Eligible Nonprofits	Examples of Ineligible Nonprofits
Faith-based organizations (churches, synagogues, mosques, or other faith-based facilities)	Nonprofits that operate government-owned buildings/facilities and/or government entities
Nonprofit healthcare facilities, private schools	Nonprofit foundations of state/public universities
Other nonprofits (community centers, museums, etc.)	Public schools



Is Your Organization Eligible?

Examples of Eligible Nonprofit Organizations*	Examples of Ineligible Organizations
Faith-based organizations (churches, synagogues, mosques, or other faith-based facilities)	Nonprofits that operate government-owned buildings/facilities and/or government entities
Nonprofit healthcare facilities	Nonprofit foundations of state/public universities
Other nonprofits (community centers, museums, etc.)	Municipal/public schools, colleges, universities, libraries
Private schools	For-profit colleges/universities
Nonprofit event venues	For-profit event venues (amusement parks, stadiums, etc.)
Camps	Utility companies
Shelters/crisis centers	Volunteer fire departments/search and rescue (SAR)

**The list shown above is not exhaustive and only provides examples of organizations that may be eligible for NSGP funding.*



How is Terrorism or Extremism Defined?

Racially or Ethnically Motivated Violent Extremists	Other Domestic Terrorism Threats
Violent extremists with ideological agendas derived from bias, often related to race or ethnicity—held by the actor against others—including a given population group.	Violent extremists with ideological agendas that are not otherwise defined under one of the other domestic terrorism threat categories. Motivations may include a combination of personal grievances and beliefs with a potential bias to religion, gender, or sexual orientation.

Demonstrating pattern of crimes that target an organization based on the criteria described in the table shown above can be used to support the ongoing threats faced by the organization.

On their own, crimes such as theft, vandalism, burglaries, and/or trespassing will not meet the definition of terrorism or extremist threats and/or attacks.



NSGP Funding Categories

NSGP – Urban Area (UA)

Organizations with facilities located within a UASI-designated high-risk urban area.

Any facility within **King, Pierce, and Snohomish** counties.

Applications compete other applications from the Seattle urban area **AND** against all NSGP-UA applications nationally.

NSGP – State

Organizations with facilities located outside of a UASI-designated high-risk urban area.

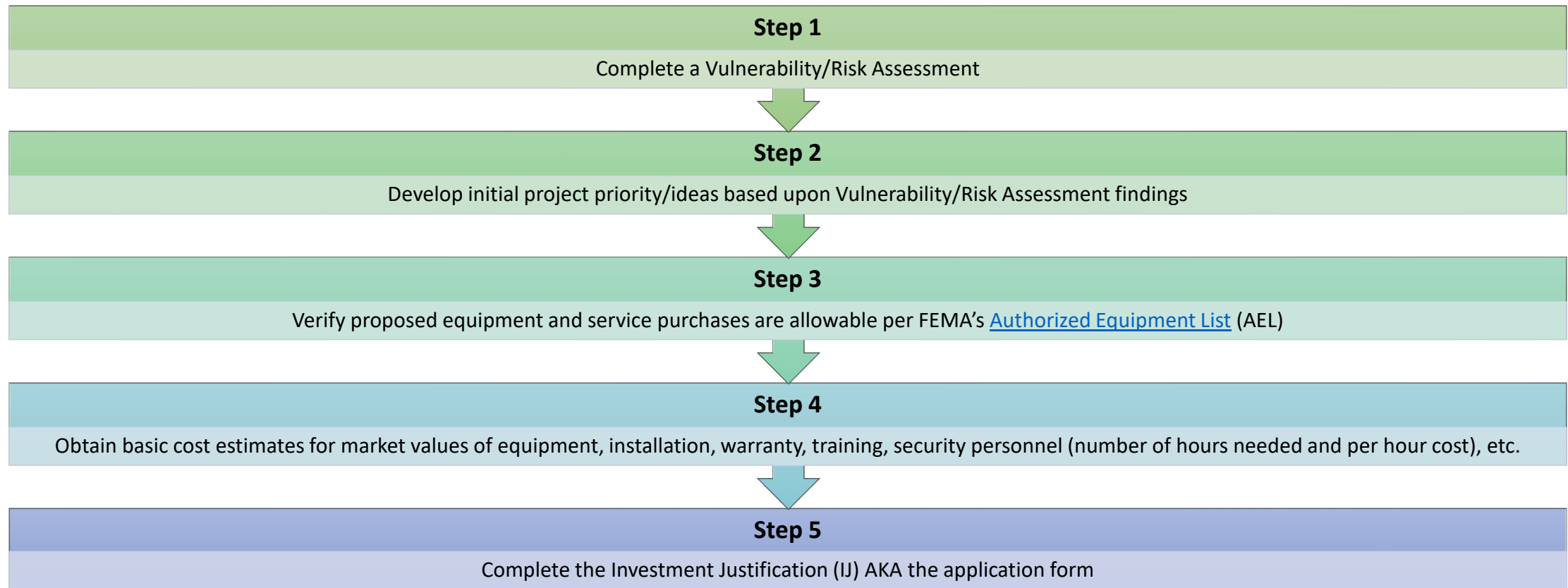
Facilities in all other Washington counties.

Applications compete among other NSGP-S applications only from within Washington State.



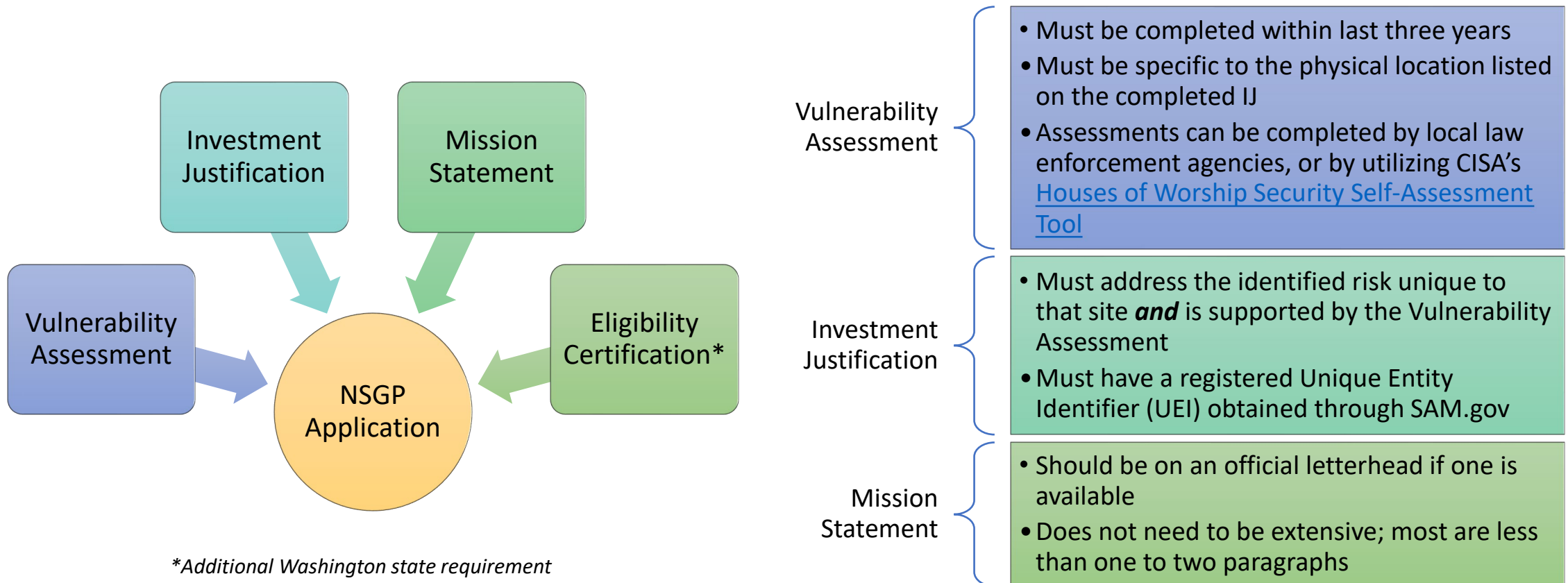


Preparing an Application





Application Components





Funding Limits

Funding Category	Max Applications Per Physical Address	Max Funding Per Application	Max Applications Per Funding Category	Max Cumulative Funding Request
NSGP – Urban Area	1	\$200,000	3	\$600,000
NSGP – State	1	\$200,000	3	\$600,000

- A nonprofit may only submit **one application per site/location/physical address**.
- Nonprofits with multiple sites (multiple locations/physical addresses) may choose to apply for additional sites at up to \$200,000 per site. Nonprofits may apply for a maximum of three sites.
- The cumulative total funding request for all applications for organizations cannot exceed \$600,000.
- **Funding limits for NSGP will be provided upon the release of the NSGP NOFO. Please visit our NSGP Applicant website for updates.**



Applying for Locations in Both Funding Categories

Funding Category	Max Applications Per Physical Address	Max Funding Per Application*	Max Total Applications	Max Cumulative Funding Request
NSGP – Urban Area <u>and</u> NSGP - State	1	\$200,000	6	\$600,000

- A nonprofit organization with sites in both NSGP-S and NSGP-UA areas may apply for a total of up to six sites, but the cumulative total of their applications cannot exceed \$600,000.
- The maximum amount requested cannot exceed \$200,000 per application.
- **Funding limits for NSGP may be updated upon the release of the NOFO. Please visit our NSGP Applicant website for updates.**



Multiple Applications – Scenario 1

	Application A	Application B	Application C	Total Amount Requested
Funding Requested	\$200,000	\$200,000	\$200,000	\$600,000
Funding Stream	NSGP-Urban Area	NSGP-State	NSGP-State	
Is this Application Eligible for Funding Consideration?	Yes	Yes	Yes	



Multiple Applications – Scenario 2

	Application A	Application B	Application C	Total Amount Requested
Funding Requested	\$300,000	\$150,000	\$150,000	\$600,000 \$300,000
Funding Stream	NSGP-State	NSGP-State	NSGP-State	
Is this Application Eligible for Funding Consideration?	NO - Exceeds maximum funding per funding request.	Yes	Yes	



Multiple Applications – Scenario 3

	Application A	Application B	Application C	Total Amount Requested
Funding Requested	\$300,000	\$300,000	-	\$600,000
Funding Stream	NSGP-Urban Area	NSGP-Urban Area	-	
Is this Application Eligible for Funding Consideration?	NO - Exceeds maximum funding per funding request.	NO - Exceeds maximum funding per funding request.	-	



Multiple Applications – Scenario 4

	Applicant A		Applicant B	
Funding Requested	\$200,000		\$200,000	
Funding Stream	NSGP-Urban Area		NSGP-Urban Area	
Physical Address	123 Main Street Monroe, WA		123 Main Street Monroe, WA	
Is this Application Eligible for Funding Consideration?	NO – Multiple applications received from one physical address.		NO - Multiple applications received from one physical address.	



How to Complete a Vulnerability Assessment

To be considered valid for the application, vulnerability assessments must be completed within the last three years.

The assessment can be completed by:

- Scheduling an in-person site assessment with your local law enforcement agency **or**
- Completing CISA's Houses of Worship Self Assessment

Applicants will need to inquire with their local law enforcement agency to determine if they can perform an in-person assessment.



America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Access Control / Entry Control

Controlling how and when staff, parishioners, visitors, and others can access the house of worship facilities and grounds is considered an effective mechanism for protecting against different threats, including active shooters. These controls can include minimizing the number of points of entry, requiring identification, or conducting searches. However, these entry controls may sometimes run counter to the overarching objective of creating an open and inviting environment for worship and fellowship. Entry controls are part of the broader layers of defense that houses of worship may have in place to enhance security. Entry controls can help deter individuals from initiating violent attacks, detect attacks earlier at a safe distance, and delay attackers from reaching vulnerable and/or highly populated locations.

To view Background, Reference, and/or More Information related to a question click the '+' icon below the options per question.

QUESTION	VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
36. Does the house of worship screen persons, bags, packages, or deliveries at the facility?	No screening takes place at the house of worship. Anything can be brought into the sanctuary, administrative areas or fellowship halls at any time without question.	No specific screening takes place; however, ushers are trained to be aware of unusual items being brought into worship areas during primary worship services. At all other times, anything can be brought into the facility.	Signs are posted that indicate no weapons are allowed. Ushers and others are trained to identify, question, screen, or prohibit items that are not otherwise identifiable (e.g., unmarked boxes, unusual or unexpected deliveries) on primary worship service days.	Signs are posted that indicate no weapons are allowed. Ushers and others trained to identify, question, screen, or prohibit items that are not otherwise identifiable (e.g., unmarked boxes, unusual or unexpected deliveries) on primary worship service days. Magnetometers are used at entry points to worship areas before and during services on primary worship service day.	Signs are posted that indicate no weapons are allowed. Specific locations for deliveries and all deliveries are inspected away from main entrances or offices. Magnetometers are used at entry points to worship areas before and during services at all times. On non-worship days, all visitors go through magnetometer screening upon entrance to any area of the house of worship (administrative areas, meeting halls, sanctuary, etc.).
	☐ Very Low	☐ Low	☐ Medium	☐ High	☐ Very High
+ Background Reference					



Vulnerability Assessments

IMPORTANT!!!

Organizations may have a private security firm complete an assessment of their facilities; however, fees incurred for these assessments cannot be included in the application.



Selecting Projects for an Application

- All projects prioritized for funding must be identified as a finding in the completed vulnerability assessment, and
- Must be allowable to be funded by NSGP according to FEMA's Authorized Equipment List (AEL)

Links and spreadsheets for FEMA's AEL can be found on our NSGP Applicant website.



Funding Priorities – First Tier

Priority Areas	Core Capabilities Enhanced	Example Project Types
National Priorities		
Enhancing the Protection of Soft Targets/Crowded Places	• Planning • Operational coordination • Public information and warning • Intelligence and Information Sharing • Interdiction and disruption • Screening, search, and detection • Access control and identity verification • Physical protective measures • Risk management for protection programs and activities • Cybersecurity • Long-term vulnerability reduction • Situational assessment • Infrastructure systems	• Private contracted security guards • Physical security enhancements • Closed circuit television (CCTV) security cameras • Security screening equipment for people and baggage • Access controls • Fencing, gates, barriers, etc. • Card readers, associated hardware/software • Cybersecurity enhancements • Risk-based cybersecurity planning and training • Improving cybersecurity of access control and identify verification systems • Improving cybersecurity of security technologies (e.g., CCTV systems) • Adoption of cybersecurity performance goals (Cross-Sector Cybersecurity Performance Goals CISA)



Funding Priorities – Second Tier

Priority Areas	Core Capabilities Enhanced	Example Project Types
Enduring Needs		
Planning	• Planning • Risk management for protection programs and activities • Risk and disaster resilience assessment • Threats and hazards identification • Operational coordination	• Conduct or enhancement of security risk assessments • Development of: • Security plans and protocols • Emergency/contingency plans • Evacuation/shelter in place plans
Training & Awareness	• Long-term vulnerability reduction • Public information and warning	• Active shooter training, including integrating the needs of persons with disabilities • Security training for employees • Public awareness/preparedness campaigns
Exercises	• Long-term vulnerability reduction	• Response exercises



Obtain Project Estimates

Once the projects are identified and prioritized and determined to be allowable for funding, begin obtaining basic cost estimates for your application.

DO NOT submit copies of these estimates with your application.

From here begin completing the Investment Justification.



Investment Justification (IJ)

Fill out the Investment Justification (IJ) form. Successful applications are those that:

- Clearly communicate threats faced from either terrorism or violent extremism
- Request funding for projects that are directly supported by a recently completed vulnerability assessment (assessments completed within the last three years)
- Request projects that are feasible and reasonable to be completed within the open period of a NSGP passthrough grant agreement

A new IJ form is released for each funding opportunity. Please visit our website after the release of the NSGP NOFO to download a copy.

DO NOT submit a prior-year version of the IJ with your application.



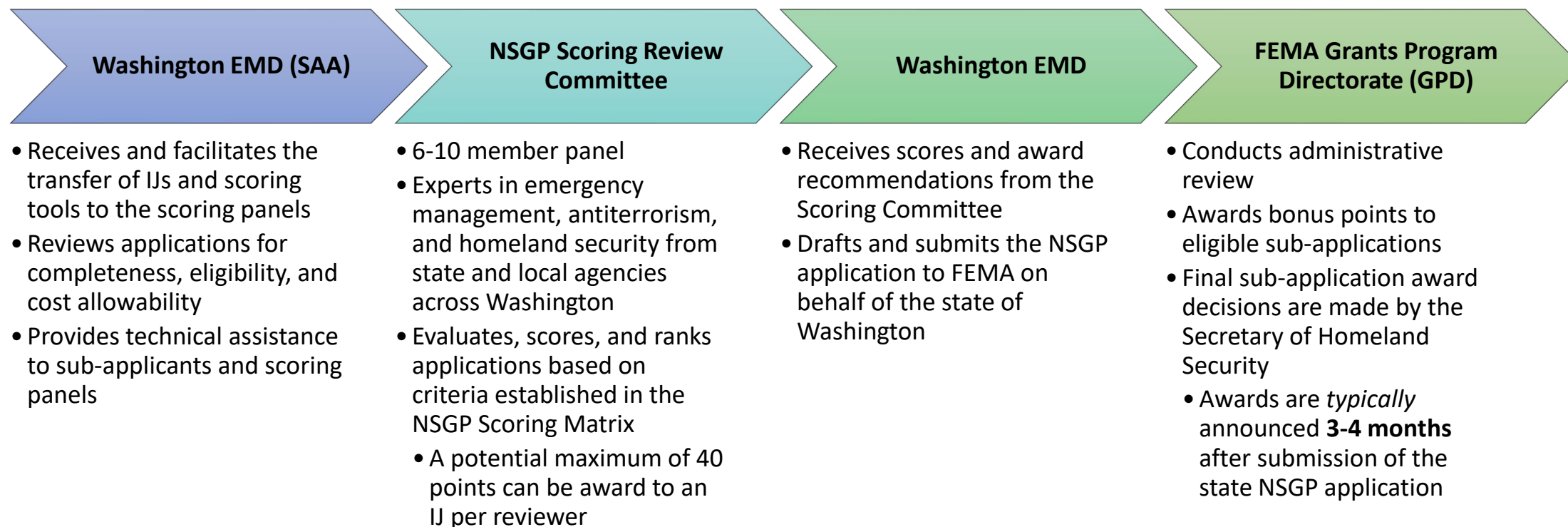
MISSION STATEMENTS

Obtain a copy of your organization's mission statement on official letterhead.*

** If official letterhead is available.*

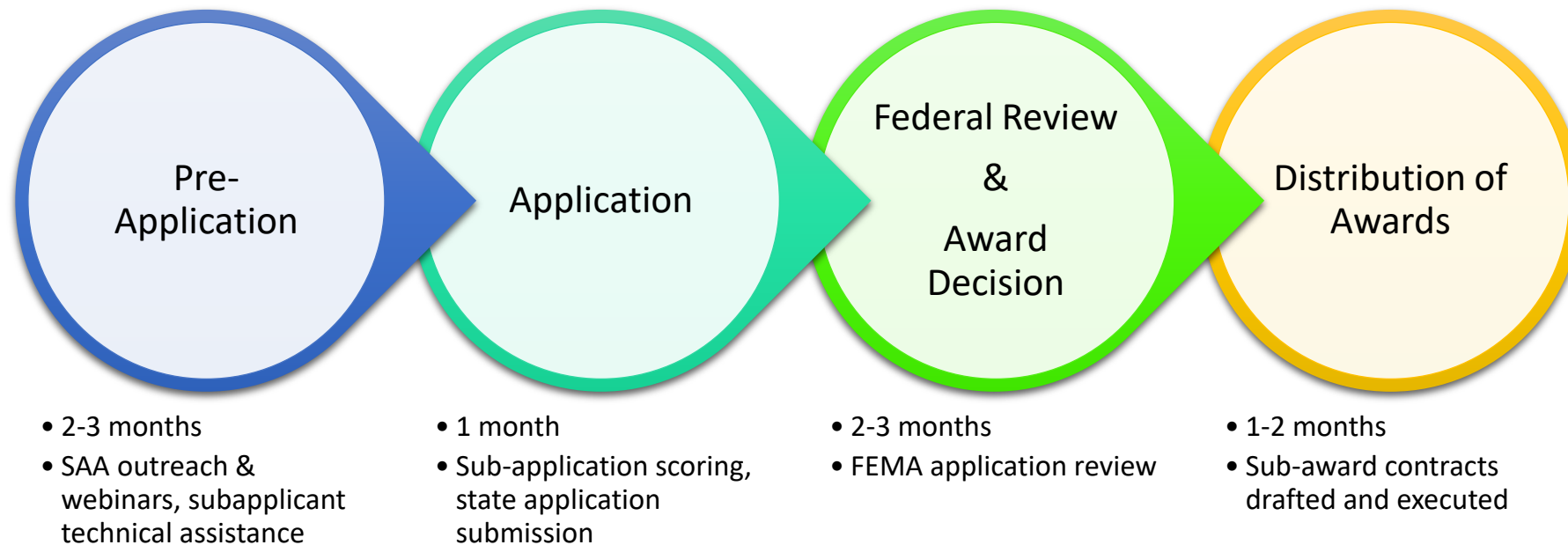


How Are Applications Reviewed





Typical Application Timeline



****The finalized timeline will be posted to our NSGP Applicant webpage upon the release of the NSGP NOFO.***



Questions?

Email all inquiries to our
Preparedness Grants main inbox.
Preparedness.Grants@mil.wa.gov

Frequently asked questions can be found on our NSGP Applicant webpage.
[Grants NSGP Application Details | Washington State Military Department,
Citizens Serving Citizens with Pride & Tradition](#)