The Department of Homeland Security (DHS)

Notice of Funding Opportunity (NOFO)

Fiscal Year 2025 Homeland Security National Training Program (HSNTP), Continuing Training Grants (CTG)

National Cybersecurity Preparedness Consortium (NCPC)

Fraud, waste, abuse, mismanagement, and other criminal or noncriminal misconduct related to this program may be reported to the Office of Inspector General (OIG) Hotline. The toll-free numbers to call are 1 (800) 323-8603 and TTY 1 (844) 889-4357.

Contents

1. Basic Information

A. Agency Name	U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA)
B. NOFO Title	Fiscal Year 2025 Homeland Security National Training Program Continuing Training Grants National Cybersecurity Preparedness Consortium (NCPC)
C. Announcement Type	Initial
D. Funding Opportunity Number	DHS-25-NPD-148-00-97

E. Assistance Listing Number	97.148
F. Expected Total Funding	$ 7.2 million
G. Anticipated Number of Awards	1 award
H. Expected Award Range	$7.2 million – $7.2 million
I. Projected Application Start Date	08/01/2025; 12:00 p.m. Eastern Time (ET)
J. Projected Application End Date	08/15/2025 11:59 p.m. Eastern Time (ET)
K. Anticipated Funding Selection Date	September 1, 2025
L. Anticipated Award Date	September 1, 2025
M. Projected Period of Performance Start Date	September 1, 2025
N. Projected Period of Performance End Date	August 31, 2028
O. Executive Summary	The Department of Homeland Security Fiscal Year (FY) 2025 Homeland Security National Training Program (HSNTP), Continuing Training Grants (CTG), National Cybersecurity Preparedness Consortium (NCPC) provides funding to the eligible applicant to develop and deliver cybersecurity training solutions to address national preparedness gaps, map training to the core capabilities, and ensure training is available and accessible to a nationwide audience. The NCPC plays an important role in the National Training and Education System (NTES), which is part of the larger National Preparedness System (the System). The System is designed to build, sustain, and deliver the core capabilities and achieve the desired outcomes identified in the National Preparedness Goal (the Goal). The Goal is "a secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate,

	respond to, and recover from the threats and hazards that pose the greatest risk." The System provides a consistent and reliable approach to support decision making, resource allocation, and measure progress toward these outcomes.
P. Agency Contact	**a. *Program Office Contact*** National Training and Education Division (NTED) maintains programmatic responsibility for the CTG program and will maintain the program management function and responsibilities throughout the life cycle of the awarded grant. Contact our NTED point of contact Ms. Jessica Sterling at (202) 212-3042 or via email to jessica.sterling@fema.dhs.gov or Mr. Samuel Phillips at Samuel.Phillips@fema.dhs.gov for additional information. **b. *FEMA Grants News*** This channel provides general information on all FEMA grant programs and maintains a comprehensive database containing key personnel contact information at the federal, state, and local levels. FEMA Grants News Team is reachable at fema-grants-news@fema.dhs.gov OR (800) 368-6498, Monday through Friday, 9:00 AM – 5:00 PM ET. **c. *Grant Programs Directorate (GPD) Award Administration Division*** GPD's Award Administration Division (AAD) provides support regarding financial matters and budgetary technical assistance. AAD can be contacted at ASK-GMD@fema.dhs.gov. **d. *FEMA Regional Offices*** FEMA Regional Offices also may provide fiscal support, including pre- and post-award administration and technical assistance. FEMA Regional Office contact information is available at https://www.fema.gov/fema-regional-contacts. **e. *Civil Rights*** Consistent with Executive Order 14173, Ending Illegal Discrimination & Restoring Merit-Based Opportunity, the FEMA Office of Civil Rights is responsible for ensuring compliance with and enforcement of federal civil rights obligations in connection with programs and services conducted by FEMA. They are reachable at FEMA-CivilRightsOffice@fema.dhs.gov. **f. *Environmental Planning and Historic Preservation***

	The FEMA Office of Environmental Planning and Historic Preservation (OEHP) provides guidance and information about the EHP review process to FEMA programs and recipients and subrecipients. Send any inquiries regarding compliance for FEMA grant projects under this NOFO to FEMA-OEHP-NOFOQuestions@fema.dhs.gov. **g. *Payment System*** FEMA uses FEMA GO for financial reporting, invoicing, and tracking payments. The Direct Deposit/Electronic Funds Transfer (DD/EFT) method of payment is used for recipients. For any questions about the system, contact the FEMA GO Helpdesk at femago@fema.dhs.gov or (877) 585-3242, Monday through Friday, 9:00 AM – 6:00 PM ET. **h. *FEMA GO*** For technical assistance with the FEMA GO system, please contact the FEMA GO Helpdesk at femago@fema.dhs.gov or (877) 585-3242, Monday through Friday, 9:00 AM – 6:00 PM ET. **i. *FEMA Preparedness Toolkit*** The FEMA Preparedness Toolkit (PrepToolkit) provides access to tools and resources needed to implement the National Preparedness System and provide a collaborative space for communities completing the Unified Reporting Tool (URT). Recipients complete and submit their Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR), and other required assessments using the PrepToolkit. For assistance, contact support@preptoolkit.fema.dhs.gov.

2. Eligibility

A. Eligible Entities/Entity Types	Only the following entities or entity types are eligible to apply. **a. *Applicants*** University of Arkansas, Criminal Justice Institute (Executive Agent for the NCPC) **b. *Subapplicants*** Subapplicants and subawards are allowed under this Funding Opportunity.

	Subapplicants should not have foreign nationals or noncitizens included. If a subapplicant has foreign nationals, they must be properly vetted and must adhere to all government statues, polices, and procedures including "staff American, stay in America" and security requirements.
B. Project Type Eligibility	**a.** ***Unallowable Project Types*** This program does not allow construction and renovation projects. **b.** ***Allowable Project Type*** • Identify current and emerging threats through Unified Training Needs Assessments to inform development of new courses and recertification to ensure communities needs are being met. • Collaborate with NCPC partners on new course offerings to ensure alignment with current gaps/needs, identify current and future risk, and avoid unneeded duplication. • Identify innovative approaches by applying new methodologies, best practices, and by leveraging new technology to improve effectiveness of the training programs.
C. Requirements for Personnel, Partners, and Other Parties	Subapplicants should not have foreign nationals or noncitizens included. If a subapplicant has foreign nationals, they must be properly vetted and must adhere to all government statues, polices, and procedures including "staff American, stay in America" and security requirements. Subapplicants/subrecipients must submit short bios and resumes. This should include the type of entity, organizational leadership, and board members along with the both the names and addresses of the individuals. Resumes are subject to approval.
D. Maximum Number of Applications	The maximum number of applications that can be submitted is: 1 per applicant.
E. Additional Restrictions	Applicants/subapplicants or recipients/subrecipients are required to certify their compliance with federal statues, DHS directives, polices, and procedures.

F. References for Eligibility Factors within the NOFO	Please see the following references provided below: 1. "Responsiveness Review Criteria" not applicable 2. "Financial Integrity Criteria" subsection C 3. "Supplemental Financial Integrity Criteria and Review" subsection D 4. FEMA may/will request financial information such as Employer Identification Number (EIN) and bank information as part of the potential award selection. This will apply to everyone prospered, including subrecipients.
G. Cost Sharing Requirement	There is no cost share requirement.
H. Cost Share Description, Type and Restrictions	Not applicable.
I. Cost Sharing Calculation Example	Not applicable
J. Required information for verifying Cost Share	Not applicable

3. Program Description

A. Background, Program Purpose, and Program History

The Continuing Training Grants (CTG) under the National Cybersecurity Preparedness Consortium (NCPC) program is a specialized initiative within the broader Homeland Security National Training Program (HSNTP). This program is specifically designed to enhance the nation's cybersecurity preparedness by providing targeted training and resources to state, local, tribal, and territorial (SLTT) governments, as well as other key stakeholders.

The CTG NCPC program was established to address the growing need for cybersecurity training and education across various levels of government and critical infrastructure sectors. With the increasing frequency and sophistication of cyber threats, there is a pressing need for comprehensive training programs that can equip personnel with the skills and knowledge necessary to protect against, respond to, and recover from cyber incidents.

Program Purpose

The primary purpose of the CTG NCPC program is to support the development and delivery of cybersecurity training that enhances the capabilities of SLTT governments and other stakeholders. This includes training on topics such as cyber threat detection and response, incident management, and cybersecurity best practices. By building these capabilities, the program aims to strengthen the overall resilience of the nation's critical infrastructure and improve the ability to respond to cyber threats.

Program History

The CTG NCPC program has evolved in response to the dynamic nature of the cybersecurity landscape. Initially focused on foundational cybersecurity training, the program has expanded to include more advanced and specialized courses that address emerging threats and technologies. Over the years, the program has also placed a greater emphasis on collaboration and information sharing among stakeholders, recognizing that a coordinated approach is essential for effective cybersecurity preparedness.

B. Goals and Objectives

The goal of the CTG NCPC program is to enable communities to address emerging cybersecurity threats and close capability gaps through development and delivery of cybersecurity learning solutions that strengthen the nation's preparedness. The NCPC identifies, develops, tests, and delivers training to state, local, tribal, and territorial (SLTT) emergency response providers, provides on-site mobile and web-based training at the awareness, performance, planning and management levels. Through collaboration, FEMA and the NCPC members address long-term cybersecurity trends that influence national preparedness—including emerging cybersecurity threats, new technologies and continuous individual, organizational, and community cybersecurity risk. The objectives of the NCPC program are to:

- Identify, develop, test, and deliver on-site mobile and web-based training at the awareness, performance, planning and management levels to SLTT emergency response providers;
- Analyze and address long-term cybersecurity trends that influence national preparedness—including emerging cybersecurity threats, new technologies and continuous individual, organizational, and community cybersecurity risk;
- Address and mitigate current and emerging cyber security capability gaps and risks.

FEMA is committed to reducing complexity, increasing efficiency, and improving outcomes. In simple terms, the training return on investment (ROI) is expressed as the benefit to cost ratio for individuals, teams, departments, jurisdictions, and regions across the nation to reach and maintain fully qualified/mission capable status. In practice, training ROI is difficult to measure. The cost of training varies significantly depending upon several variables including delivery format (i.e., online, indirect/train-the-trainer, mobile, resident/on-campus) and competency level

(i.e., performance, management, and planning). FEMA uses a systematic approach to optimize the national preparedness training portfolio, align resources to address capability gaps through the most effective and efficient means available, and ensure a sound ROI from the local to the national level. NCPC collaboration with the FEMA training enterprise is integral to that effort.

C. Program Rationale

The CTG NCPC program aims to achieve its goals and objectives through a structured approach that includes developing and delivering FEMA-certified training solutions to build and sustain the capabilities of emergency responders. This program aligns with the FY 2023 Quadrennial Homeland Security Review (QHSR) through:

Achieving Goals and Objectives

1. **Training Development and Delivery**: The program focuses on creating and providing mission critical and mission essential training that helps emergency responders before, during, and after disasters.
2. **Addressing Preparedness Gaps**: By targeting specific gaps in preparedness and response capabilities, the program ensures a more integrated and risk-informed approach to emergency management.
3. **Strengthening the Emergency Management Workforce**: Aligning with the DHS's emphasis on building a skilled and ready workforce.
4. **Promoting Innovation**: Integrating advanced cybersecurity into emergency response operations, which aligns with the DHS's focus on leveraging technology to enhance security and resilience.

D. Federal Assistance Type

The CTG NCPC program, prescribed by this NOFO, is awarded through a separate cooperative agreement, as defined by, and consistent with the Federal Grant and Cooperative Agreement Act of 1977 (Pub. L. No. 95-244, 31 U.S.C. §§ 6301-6308). FEMA maintains substantial involvement with the recipient as it carries out activities under the award to include financial monitoring and all training development and delivery activities, including the creation and approval of course content, arrangement of learning objectives, establishment of training delivery modes and methods, and use of the Kirkpatrick evaluation model. NTED Training Partners Program (TPP) managers serve as the authority to provide approval and disapproval for all activities over the life cycle of the award.

E. Performance Measures and Targets

NCPC members are required to collect data to allow FEMA to measure performance and outcomes. FEMA will measure the NCPC members' performance using the following indicators:

1. In order to demonstrate good financial stewardship, the NCPC and FEMA will evaluate the direct cost per student.
2. In order to measure how well the grant helps strengthen preparedness through training NCPC members will use Kirkpatrick level 1, 2, and 3 evaluations.
    - Level 1 surveys will be utilized to determine how well the training met student needs with a target goal of at least 75% of respondents indicating satisfaction or greater.
    - Level 2 assessments compare pre- and post-test results to determine how much students learned with a target of an overall average of 26-point increase.
    - Level 3 assessments are used to measure to what degree students are applying the knowledge and skills gained through training to their roles within their home jurisdiction.

F. Program-Specific Unallowable Costs

This program does not allow construction and renovation costs and is subject to all Terms & Conditions where restrictions are provided.

G. General Funding Requirements

Costs charged to federal awards (including federal and non-federal cost share funds) must comply with applicable statutes, rules and regulations, policies, this NOFO, and the terms and conditions of the federal award. This includes, among other requirements, that costs must be incurred, and products and services must be delivered within the budget period. 2 C.F.R. § 200.403(h).

Recipients may not use federal funds or any cost share funds for the following activities:

1. Matching or cost sharing requirements for other federal grants and cooperative agreements (see 2 C.F.R. § 200.306).
2. Lobbying or other prohibited activities under 18 U.S.C § 1913 or 2 C.F.R. § 200.450.
3. Prosecuting claims against the federal government or any other government entity (see 2 C.F.R. § 200.435).

H. Indirect Costs (Facilities and Administrative Costs)

Indirect costs (IDC) are allowable under this opportunity for costs incurred for a common or joint purpose benefitting more than one cost objective and not readily assignable to specific cost objectives without disproportionate effort. Applicants with a current negotiated IDC rate agreement who desire to charge indirect costs to a federal award must provide a copy of their IDC rate agreement with their applications. Not all applicants are required to have a current negotiated IDC rate agreement. Applicants that are not required to have a negotiated IDC rate agreement, but are required to develop an IDC rate proposal, must provide a copy of their

proposal with their applications. Applicants without a current negotiated IDC rate agreement (including a provisional rate) and wish to charge the de minimis rate must reach out to FEMA for further instructions. Applicants who wish to use a cost allocation plan in lieu of an IDC rate proposal must reach out to FEMA for further instructions. As it relates to the IDC for subrecipients, a recipient must follow the requirements of 2 C.F.R. §§ 200.332 and 200.414 in approving the IDC rate for subawards.

I. Management and Administration (M&A) Costs

M&A costs are allowed at no greater than 5% of award.

M&A are not overhead costs but are necessary direct costs incurred in direct support of the federal award or as a consequence of it, such as travel, meeting-related expenses, and salaries of full/part-time staff in direct support of the program. As such, M&A costs can be itemized in financial reports.

J. Pre-Award Costs

Pre-award costs are not allowed.

K. Beneficiary Eligibility

Not applicable.

This NOFO and any subsequent federal awards create no rights or causes of action for any beneficiary.

L. Participant Eligibility

Not applicable

This NOFO and any subsequent federal awards create no rights or causes of action for any participant.

M. Authorizing Authority

National Cybersecurity Preparedness Consortium Act, 2021 (Pub. L. No. 117-122)

N. Appropriation Authority

Full-Year Continuing Appropriations and Extensions Act, 2025, Pub L. No. 119-4, § 1101.

O. Budget Period

There will be only a single budget period with the same start and end dates as the period of performance.

4. Application Contents and Format

A. Pre-Application, Letter of Intent, and Whitepapers
Not applicable.

B. Application Content and Format
Please refer to Appendix A of this NOFO.

C. Application Components
The following forms or information are required to be submitted via FEMA GO. The Standard Forms (SF) are also available at Forms | Grants.gov.

- SF-424, Application for Federal Assistance
- Grants.gov Lobbying Form, Certification Regarding Lobbying
- SF-LLL, Disclosure of Lobbying Activities

D. Program-Specific Required Documents and Information
The following program-specific forms or information are required to be submitted in FEMA GO:

- Please refer to Appendix A of this NOFO.

E. Post-Application Requirements for Successful Applicants
Not applicable.

F. Prohibition on Covered Equipment or Services
Recipients, sub-recipients, and their contractors or subcontractors must comply with the prohibitions set forth in Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which restrict the purchase of covered telecommunications and surveillance equipment and services. Please see 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200, and FEMA Policy #405-143-1 - Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services for more information.

5. Submission Requirements and Deadlines

A. Address to Request Application Package
Applications are processed through the FEMA GO system. To access the system, go to https://go.fema.gov/.

Steps Required to Apply for an Award under this program and Submit an Application:

To apply for an award under this program, all applicants must:

a. Apply for, update, or verify their Unique Entity Identifier (UEI) number and EIN from the Internal Revenue Service;
b. In the application, provide an UEI number;
c. Have an account with login.gov;
d. Register for, update, or verify their System for Award Management (SAM) account and ensure the account is active before submitting the application;
e. Register in FEMA GO, add the organization to the system, and establish the Authorized Organizational Representative (AOR). The organization's electronic business point of contact (eBiz POC) from the SAM registration may need to be involved in this step. For step-by-step instructions, see https://www.fema.gov/media-library/assets/documents/181607;
f. Submit the complete application in FEMA GO; and
g. Continue to maintain an active SAM registration with current information at all times during which it has an active federal award or an application or plan under consideration by a federal awarding agency. As part of this, applicants must also provide information on an applicant's immediate and highest-level owner and subsidiaries, as well as on all predecessors that have been awarded federal contracts or federal financial assistance within the last three years, if applicable.

Per 2 C.F.R. § 25.110(a)(2)(iv), if an applicant is experiencing exigent circumstances that prevents it from obtaining an UEI number and completing SAM registration prior to receiving a federal award, the applicant must notify FEMA as soon as possible. Contact fema-grants-news@fema.dhs.gov and provide the details of the exigent circumstances.

How to Register to Apply:

General Instructions:

Registering and applying for an award under this program is a multi-step process and requires time to complete. Below are instructions for registering to apply for FEMA funds. Read the instructions carefully and prepare the requested information before beginning the registration process. Gathering the required information before starting the process will alleviate last-minute searches for required information.

The registration process can take up to four weeks to complete. To ensure an application meets the deadline, applicants are advised to start the required steps well in advance of their submission.

Organizations must have a UEI number, EIN, and an active SAM registration.

Obtain a UEI Number:

All entities applying for funding, including renewal funding, must have a UEI number. Applicants must enter the UEI number in the applicable data entry field on the SF-424 form. For more detailed instructions for obtaining a UEI number, refer to SAM.gov.

Obtain Employer Identification Number:

In addition to having a UEI number, all entities applying for funding must provide an EIN. The EIN can be obtained from the IRS by visiting https://www.irs.gov/businesses/small-businesses-self-employed/apply-for-an-employer-identification-number-ein-online.

Create a login.gov account:

Applicants must have a login.gov account in order to register with SAM or update their SAM registration. Applicants can create a login.gov account at: https://secure.login.gov/sign_up/enter_email?request_id=34f19fa8-14a2-438c-8323-a62b99571fd.

Applicants only have to create a login.gov account once. For existing SAM users, use the same email address for both login.gov and SAM.gov so that the two accounts can be linked.

For more information on the login.gov requirements for SAM registration, refer to https://www.sam.gov/SAM/pages/public/loginFAQ.jsf.

Register with SAM:

In addition to having a UEI number, all organizations must register with SAM. Failure to register with SAM will prevent your organization from applying through FEMA GO. SAM registration must be renewed annually and must remain active throughout the entire grant life cycle.

For more detailed instructions for registering with SAM, refer to: Register with SAM

Note: per 2 C.F.R. § 25.200, applicants must also provide the applicant's immediate and highest-level owner, subsidiaries, and predecessors that have been awarded federal contracts or federal financial assistance within the past three years, if applicable.

Register in FEMA GO, Add the Organization to the System, and Establish the AOR:

Applicants must register in FEMA GO and add their organization to the system. The organization's electronic business point of contact (eBiz POC) from the SAM registration may need to be involved in this step. For step-by-step instructions, see: FEMA GO Startup Guide.

Note: FEMA GO will support only the most recent major release of the following browsers:

Google Chrome;

Mozilla Firefox;

Apple Safari; and

Microsoft Edge.

Applicants using tablet type devices or other browsers may encounter issues with using FEMA GO.

Submitting the Final Application:

Applicants will be prompted to submit the standard application information, and any program-specific information required. Standard Forms (SF) may be accessed in the Forms tab under the: SF-424 Family | Grants.gov.

Applicants should review these forms before applying to ensure they are providing all required information.

After submitting the final application, FEMA GO will provide either an error message, or an email to the submitting AOR confirming the transmission was successfully received.

B. Application Deadline
08/15/2025 11:59 p.m. Eastern Time (ET)

C. Pre-Application Requirements Deadline
Not applicable

D. Post-Application Requirements Deadline
Not applicable

E. Effects of Missing the Deadline
All applications must be completed in FEMA GO by the application deadline. FEMA GO automatically records proof of submission and generates an electronic date/time stamp when FEMA GO successfully receives an application. The submitting AOR will receive via email the official date/time stamp and a FEMA GO tracking number to serve as proof of timely submission prior to the application deadline.

Applicants experiencing system-related issues have until 3:00 PM ET on the date applications are due to notify FEMA. No new system-related issues will be addressed after this deadline. Applications not received by the application submission deadline will not be accepted.

6. Intergovernmental Review

A. Requirement Description and State Single Point of Contact
An intergovernmental review may be required. Applicants must contact their state's Single Point of Contact (SPOC) to comply with the state's process under Executive Order 12372.

7. Application Review Information

A. Threshold Criteria

1. Application Evaluation Criteria

    a. This notice provides funding for the NCPC partners to develop, deliver, and evaluate mission critical and mission essential training for state, local, tribal and territorial partners, which supports the objective of the National Preparedness System to facilitate an integrated, community-centric, risk-informed, capabilities-based approach to preparedness.

B. Application Criteria

Programmatic Criteria

1. **Technical Merit**

    The proposal will be reviewed and evaluated on an applicant's understanding of the topic based upon statements provided in the narrative that describe knowledge of the topic to include an awareness of current and emerging issues.

2. **National in Scope**

    FEMA will review the proposal to determine the number and range of locations and communities directly and indirectly impacted according to the proposal.

3. **Target Audience**

    FEMA will review the proposal to determine whether the proposed training identifies and links to the target audience.

4. **Training Development and Plan**

    FEMA will review the proposal to determine if the training plan correctly incorporates the Instructional System Design, Analysis Design Development Implementation Evaluation (ISD ADDIE) model.

5. **Budget**

    FEMA will review the budget to determine whether an applicant addressed all categories and elements with dollar amounts and justifications as appropriate.

C. Financial Integrity Criteria

Before making an award, FEMA is required to review OMB-designated databases for applicants' eligibility and financial integrity information. This is required by the Payment Integrity Information Act of 2019 (Pub. L. No. 116-117, § 2 (2020)), 41 U.S.C. § 2313, and the "Do Not Pay Initiative" (31 U.S.C. 3354). For more details, please see 2 C.F.R. § 200.206.

Thus, the Financial Integrity Criteria may include the following risk-based considerations of the applicant:

1. Financial stability.
2. Quality of management systems and ability to meet management standards.
3. History of performance in managing federal award.
4. Reports and findings from audits.
5. Ability to effectively implement statutory, regulatory, or other requirements.

D. Supplemental Financial Integrity Criteria and Review

Before making an award expected to exceed the simplified acquisition threshold (currently a total federal share of $250,000) over the period of performance:

FEMA is required by 41 U.S.C. § 2313: to review or consider certain information found in SAM.gov. For details, please see 2 C.F.R. § 200.206(a)(2).

1. An applicant may review and comment on any information in the responsibility/qualification records available in SAM.gov.
2. Before making decisions in the risk review required by 2 C.F.R. § 200.206, FEMA will consider any comments by the applicant.

E. Reviewers and Reviewer Selection

The Deputy Administrator, FEMA Resilience, will approve or disapprove the statements of work proposed by the NCPC and submit award recommendations through the FEMA Administrator to the Secretary of Homeland Security.

F. Merit Review Process

There is no merit review process for these non-competitive awards.

G. Final Selection
The Deputy Administrator, FEMA Resilience, will approve or disapprove the awards proposed by the NCPC and submit award recommendations through the FEMA Administrator to the Secretary of Homeland Security.

8. Award Notices

A. Notice of Award

The Authorized Organization Representative should carefully read the federal award package before accepting the federal award. The federal award package includes instructions on administering the federal award as well as terms and conditions for the award.

By submitting an application, applicants agree to comply with the prerequisites stated in this NOFO and the material terms and conditions of the federal award, should they receive an award.

Before accepting the award, the AOR and recipient should carefully read the award package. The award package includes instructions on administering the grant award and the terms and conditions associated with responsibilities under federal awards. Recipients must accept all conditions in this NOFO.

FEMA will provide the federal award package to the applicant electronically via FEMA GO. Award packages include an Award Letter, Summary Award Memo, Agreement Articles, and Obligating Document. An email notification of the award package will be sent through FEMA's grant application system to the AOR that submitted the application.

NCPC must accept their awards no later than 30 days from the award date. The recipient shall notify FEMA of its intent to accept and proceed with work under the award through the FEMA GO system.

Funds will remain on hold until the recipient accepts the award through the FEMA GO system and all other conditions of the award have been satisfied or until the award is otherwise rescinded. Failure to accept a grant award within the specified timeframe may result in a loss of funds.

B. Pass-Through Requirements
Not applicable

C. Note Regarding Pre-Award Costs
Not applicable

Even if pre-award costs are allowed, beginning performance is at the applicant and/or sub-applicant's own risk.

D. Obligation of Funds
Funds will not be made available for obligation, expenditure, or drawdown until the applicant's budget (to include Indirect Cost Agreement, if applicable) and budget narrative have been approved by FEMA and the grant award accepted by the recipient.

9. Post-Award Requirements and Administration

A. Administrative and National Policy Requirements

Presidential Executive Orders

Recipients must comply with the requirements of Presidential Executive Orders related to grants (also known as federal assistance and financial assistance), the full text of which are incorporated by reference.

In accordance with Executive Order 14305, Restoring American Airspace Sovereignty (June 6, 2025), and to the extent allowed by law, eligible state, local, tribal, and territorial grant recipients under this NOFO are permitted to purchase unmanned aircraft systems, otherwise known as drones, or equipment or services for the detection, tracking, or identification of drones and drone signals, consistent with the legal authorities of state, local, tribal, and territorial agencies. Recipients must comply with all applicable federal, state, and local laws and regulations, and adhere to any statutory requirements on the use of federal funds for such unmanned aircraft systems, equipment, or services.

Subrecipient Monitoring and Management

Pass-through entities must comply with the requirements for subrecipient monitoring and management as set forth in 2 C.F.R. §§ 200.331-33.

B. DHS Standard Terms and Conditions

A recipient under this funding opportunity must comply with the DHS Standard Terms and Conditions in effect as of the date of the federal award. The DHS Standard Terms and Conditions are available online: DHS Standard Terms and Conditions | Homeland Security. For continuation awards, the terms and conditions for the initial federal award will apply unless otherwise specified in the terms and conditions of the continuation award. The specific version of the DHS Standard Terms and Conditions applicable to the federal award will be in the federal award package.

A recipient under this funding opportunity must comply with the FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025), with the exception Paragraph C.IX (Communication and Cooperation with the Department of Homeland Security and Immigration Officials) and paragraph C.XVII(2)(a)(iii) (Anti-Discrimination Grant Award Certification regarding immigration). Paragraphs C.IX and C.XVII(2)(a)(iii) do not apply to any federal award under this funding opportunity. The FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025) are available at www.dhs.gov/publication/dhs-standard-terms-and-conditions.

C. Financial Reporting Requirements

1. Recipients must report obligations and expenditures through a federal financial report. The Federal Financial Report (FFR) form, also known as Standard Form 425 (SF-425), is available online at: SF-425 OMB #4040-0014.

2. Recipients must submit the FFR quarterly throughout the period of performance (POP) as detailed below:

3. The final FFR is due within 120 calendar days after the end of the POP.

FEMA may withhold future federal awards and cash payments if the recipient does not submit timely financial reports, or the financial reports submitted demonstrate lack of progress or provide insufficient detail.

D. Programmatic Performance Reporting Requirements

Recipients are responsible for providing updated performance reports in Microsoft Word on a semi-annual basis. These is no prescribed government form for this report. The report is due within 30 days after the end of the reporting period.

The semi-annual Performance Progress Report must follow the guidance provided by FEMA's National Training and Education Division (NTED) in the NTED Monitoring Policy and Procedure Guide. FEMA/NTED will provide this guide to recipients of a FY 2025 NDPC award as a post-award action.

E. Closeout Reporting Requirements
Within 120 days after the end of the period of performance, or after an amendment has been issued to close out a federal award, recipients must submit the following:

1. The final request for payment, if applicable.

2. The final FFR.

3. The final progress report detailing all accomplishments.

4. A qualitative narrative summary of the impact of those accomplishments throughout the period of performance.

5. Other documents required by this NOFO, terms and conditions of the federal award, or other DHS Component guidance.

After FEMA approves these reports, it will issue a closeout notice. The notice will indicate the period of performance as closed, list any remaining funds to be de-obligated, and address the record maintenance requirement. Unless a longer period applies, such as due to an audit or litigation, for equipment or real property used beyond the period of performance, or due to other circumstances outlined in 2 C.F.R. § 200.334, this maintenance requirement is three years from the date of the final FFR.

Also, pass-through entities are responsible for closing out those subawards as described in 2 C.F.R. § 200.344; subrecipients are still required to submit closeout materials within 90 calendar days of the subaward period of performance end date. When a subrecipient completes all closeout requirements, pass-through entities must promptly complete all closeout actions in time for the recipient to submit all necessary documentation and information to FEMA during the

closeout of their prime award. The recipient is responsible for returning any balances of unobligated or unliquidated funds that have been drawn down that are not authorized to be retained per 2 C.F.R. § 200.344(e).

Administrative Closeout

Administrative closeout is a mechanism for FEMA to unilaterally execute closeout of an award. FEMA will use available award information in lieu of final recipient reports, per 2 C.F.R. § 200.344(h)-(i). It is an activity of last resort, and if FEMA administratively closes an award, this may negatively impact a recipient's ability to obtain future funding.

Additional Reporting Requirements

Anytime there is a chance in personnel for any of the awardees and/or subrecipients, their information needs to be submitted for approval (all the previous personal information identified).

F. Disclosing Information per 2 C.F.R. § 180.335

Before entering into a federal award, the applicant must notify FEMA if it knows that the applicant or any of the principals (as defined at 2 C.F.R. § 180.995) for the federal award:

1. Are presently excluded or disqualified;
2. Have been convicted within the preceding three years of any of the offenses listed in § 180.800(a) or had a civil judgment rendered against you for one of those offenses within that time period;
3. Are presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State, or local) with the commission of any of the offenses listed in § 180.800(a); or
4. Have had one or more public transactions (Federal, State, or local) terminated within the preceding three years for cause or default.

This requirement is fully described in 2 C.F.R. §180.335.

Additionally, 2 C.F.R. § 180.350 requires recipients to provide immediate notice to FEMA at any time after entering a federal award if:

1. The recipient learns that either it failed to earlier disclose information as required by 2 C.F.R. § 180.335;
2. Due to changed circumstances, the applicant or any of the principals for the federal award now meet the criteria at 2 C.F.R. § 180.335 listed above.

G. Reporting of Matters Related to Recipient Integrity and Performance

Appendix XII to 2 C.F.R. Part 200 states the terms and conditions for recipient integrity and performance matters used for this funding opportunity.

If the total value of all active federal grants, cooperative agreements, and procurement contracts for a recipient exceeds $10,000,000 at any time during the period of performance:

1. The recipient must maintain the currency of information reported in SAM.gov about civil, criminal, or administrative proceedings described in paragraph 2 of Appendix XII;
2. The required reporting frequency is described in paragraph 4 of Appendix XII.

H. Single Audit Report

A recipient expending $1,000,000 or more in federal awards (as defined by 2 C.F.R. § 200.1) during its fiscal year must undergo an audit. This may be either a single audit complying with 2 C.F.R. § 200.514 or a program-specific audit complying with 2 C.F.R. §§ 200.501 and 200.507. Audits must follow 2 C.F.R. Part 200, Subpart F, 2 C.F.R. § 200.501, and the U.S. Government Accountability Office (GAO) Generally Accepted Government Auditing Standards.

I. Monitoring and Oversight

Per 2 C.F.R. § 200.337, DHS and its authorized representatives have the right of access to any records of the recipient or subrecipient pertinent to a Federal award to perform audits, site visits, and any other official use. The right also includes timely and reasonable access to the recipient's or subrecipient's personnel for the purpose of interview and discussion related to such documents or the Federal award in general.

Pursuant to this right and per 2 C.F.R. § 200.329, DHS may conduct desk reviews and make site visits to review and evaluate project accomplishments and management control systems as well as provide any required technical assistance. Recipients and subrecipients must respond in a timely and accurate manner to DHS requests for information relating to a federal award.

J. Program Evaluation

Title I of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435 (2019) (Evidence Act), PUBL435.PS urges federal agencies to use program evaluation as a critical tool to learn, improve delivery, and elevate program service and delivery across the program lifecycle. Evaluation means "an assessment using systematic data collection and analysis of one or more programs, policies, and organizations intended to assess their effectiveness and efficiency." Evidence Act, § 101 (codified at 5 U.S.C. § 311). OMB A-11, Section 290 (Evaluation and Evidence-Building Activities) further outlines the standards and practices for evaluation activities. Federal agencies are required to specify any requirements for recipient participation in program evaluation activities (2 C.F.R. § 200.301). Program evaluation activities incorporated from the outset in the NOFO and program design and implementation allow recipients and agencies to meaningfully document and measure progress and achievement towards program goals and objectives, and identify program outcomes and lessons learned, as part of demonstrating recipient performance (2 C.F.R. § 200.301).

As such, recipients and subrecipients are required to participate in a Program Office (PO) or a DHS Component-led evaluation, if selected. This may be carried out by a third-party on behalf

of the PO or the DHS Component. Such an evaluation may involve information collections including but not limited to, records of the recipients; surveys, interviews, or discussions with individuals who benefit from the federal award, program operating personnel, and award recipients; and site visits or other observation of recipient activities, as specified in a DHS Component or PO-approved evaluation plan. More details about evaluation requirements may be provided in the federal award, if available at that time, or following the award as evaluation requirements are finalized. Evaluation costs incurred during the period of performance are allowable costs (either as direct or indirect) in accordance with 2 C.F.R. § 200.413.

Recipients and subrecipients are also encouraged, but not required, to participate in any additional evaluations after the period of performance ends, although any costs incurred to participate in such evaluations are not allowable and may not be charged to the federal award.

K. Additional Performance Reporting Requirements

Not applicable.

L. Termination of a Federal Award by FEMA

1. Paragraph C.XL of the FY 2025 DHS Standard Terms and Conditions, v.3 sets forth a term and condition entitled "Termination of a Federal Award." The termination provision condition listed below applies to the grant award and the term and condition in Paragraph C.XL of the FY 2025 DHS Standard Terms and Conditions, v.3 does not.
2. Termination of Federal Award by FEMA

   FEMA may terminate the federal award in whole or in part for one of the following reasons identified in 2 C.F.R. § 200.340:

   a. If the recipient or subrecipient fails to comply with the terms and conditions of the federal award.
   b. With the consent of the recipient, in which case FEMA and the recipient must agree upon the termination conditions. These conditions include the effective date and, in the case of partial termination, the portion to be terminated.
   c. If the federal award no longer effectuates the program goals or agency priorities. Under this provision, FEMA may terminate the award for these purposes for any of the following reasons apply:
      i. If DHS/FEMA, in its sole discretion, determines that a specific award objective is ineffective at achieving program goals as described in this NOFO;
      ii. If DHS/FEMA, in its sole discretion, determines that an objective of the award as described in this NOFO will be ineffective at achieving program goals or agency priorities;
      iii. If DHS/FEMA, in its sole discretion, determines that the design of the grant program is flawed relative to program goals or agency priorities;

iv. If DHS/FEMA, in its sole discretion, determines that the grant program is not aligned to either the DHS Strategic Plan, the FEMA Strategic Plan, or successor policies or documents;
v. If DHS/FEMA, in its sole discretion, changes or re-evaluates the goals or priorities of the grant program; and determines that the award will be ineffective at achieving the updated program goals or agency priorities or;
vi. For other reasons based on program goals or agency priorities described in the termination notice provided to the recipient pursuant to 2 C.F.R. § 200.341.
vii. If the awardee falls out of compliance with the Agency's statutory or regulatory authority, award terms and conditions, or other applicable laws.

3. Termination of a Subaward by the Pass-Through Entity

   The pass-through entity may terminate a subaward in whole or in part for one of the following reasons identified in 2 C.F.R. § 200.340:

   a. If the subrecipient fails to comply with the terms and conditions of the federal award.
   b. With the consent of the subrecipient, in which case the pass-through entity and the subrecipient must agree upon the termination conditions. These conditions include the effective date and, in the case of partial termination, the portion to be terminated.
   c. If the pass-through entities award has been terminated, the pass-through recipient will terminate its subawards.

4. Termination by the Recipient or Subrecipient

   The recipient or subrecipient may terminate the federal award in whole or in part for the following reason identified in 2 C.F.R. § 200.340: Upon sending FEMA or pass-through entity a written notification of the reasons for such termination, the effective date, and, in the case of partial termination, the portion to be terminated. However, if FEMA or pass-through entity determines that the remaining portion of the federal award will not accomplish the purposes for which the federal award was made, FEMA or the pass-through entity may terminate the federal award in its entirety.

5. Impacts of Termination
   a. When FEMA terminates the federal award prior to the end of the period of performance due to the recipient's material failure to comply with the terms and conditions of the federal award, FEMA will report the termination in SAM.gov in the manner described at 2 C.F.R. § 200.340(c).
   b. When the federal award is terminated in part or its entirety, FEMA or the pass-through entity and recipient or subrecipient remain responsible for compliance with the requirements in 2 C.F.R. §§ 200.344 and 200.345.

6. Notification requirements

FEMA or the pass-through entity must provide written notice of the termination in a manner consistent with 2 C.F.R. § 200.341. The federal award will be terminated on the date of the notification unless stated otherwise in the notification.

7. Opportunities to Object and Appeals

Where applicable, when FEMA terminates the federal award, the written notification of termination will provide the opportunity and describe the process to object and provide information challenging the action, pursuant to 2 C.F.R. § 200.342.

8. Effects of Suspension and Termination

The allowability of costs to the recipient or subrecipient resulting from financial obligations incurred by the recipient or subrecipient during a suspension or after the termination of a federal award are subject to 2 C.F.R. 200.343.

M. Best Practices

While not a requirement in the DHS Standard Terms and Conditions, as a best practice: Entities receiving funds through this program should ensure that cybersecurity is integrated into the design, development, operation, and maintenance of investments that impact information technology (IT) and/ or operational technology (OT) systems. Additionally, "The recipient and subrecipient must take reasonable cybersecurity and other measures to safeguard information including protected personally identifiable information (PII) and other types of information." 2 C.F.R. § 200.303(e).

N. Payment Information

Recipients will submit payment requests in FEMA GO for FY25 awards under this program.

Instructions to Grant Recipients Pursuing Payments

FEMA reviews all grant payments and obligations to ensure allowability in accordance with 2 C.F.R. § 200.305. These measures ensure funds are disbursed appropriately while continuing to support and prioritize communities who rely on FEMA for assistance. Once a recipient submits a payment request, FEMA will review the request. If FEMA approves a payment, recipients will be notified by FEMA GO and the payment will be delivered pursuant to the recipients SAM.gov financial information. If FEMA disapproves a payment, FEMA will inform the recipient.

Processing and Payment Timeline

FEMA must comply with regulations governing payments to grant recipients. See 2 C.F.R. § 200.305. For grant recipients other than States, 2 C.F.R. § 200.305(b)(3) stipulates that FEMA is to make payments on a reimbursement basis within 30 days after receipt of the payment request, unless FEMA reasonably believes the request to be improper. For state recipients, 2 C.F.R. § 200.305(a) instructs that federal grant payments are governed by Treasury-State Cash Management Improvement Act (CMIA) agreements ("Treasury-State agreement") and default procedures codified at 31 C.F.R. part 205 and Treasury Financial Manual (TFM) 4A-2000, "Overall Disbursing Rules for All Federal Agencies." See 2 C.F.R. § 200.305(a)2.

Treasury-State agreements generally apply to "major federal assistance programs" that are governed by 31 C.F.R. part 205, subpart A and are identified in the Treasury-State agreement. 31 C.F.R. §§ 205.2, 205.6. Where a federal assistance (grant) program is not governed by subpart Payment and funds transfers from FEMA to the state are subject to 31 C.F.R. part 205, subpart B. Subpart B requires FEMA to "limit a funds transfer to a state to the minimum amounts needed by the state and must time the disbursement to be in accord with the actual, immediate cash requirements of the state in carrying out a federal assistance program or project. The timing and amount of funds transfers must be as close as is administratively feasible to a state's actual cash outlay for direct program costs and the proportionate share of any allowable indirect costs." 31 C.F.R. § 205.33(a). Nearly all FEMA grants are not "major federal assistance programs." As a result, payments to states for those grants are subject to the "default" rules of 31 C.F.R. part 205, subpart B.

If additional information is needed, a request for information will be issued by FEMA to the recipient; recipients are strongly encouraged to respond to any additional FEMA request for information inquiries within three business days. If an adequate response is not received, the request may be denied, and the entity may need to submit a new reimbursement request; this will re-start the 30-day timeline.

Submission Process

All non-disaster grant program reimbursement requests must be reviewed and approved by FEMA prior to drawdowns.

For all non-disaster reimbursement requests (regardless of system), please ensure submittal of the following information:

1. Grant ID / Award Number
2. Total amount requested for drawdown
3. Purpose of drawdown and timeframe covered (must be within the award performance period)
4. Subrecipient Funding Details (if applicable).
    - Is funding provided directly or indirectly to a subrecipient?

- If **no,** include statement "This grant funding is not being directed to subrecipients."
- If **yes**, provide the following details:
  - The name, mission statement, and purpose of each subrecipient receiving funds, along with the amount allocated and the specific role or activity being reimbursed.
  - Whether the subrecipient's work or mission involves supporting aliens, regardless of whether FEMA funds support such activities.
  - Whether the payment request includes an activity involving support to aliens.
  - Whether the subrecipient has any diversity, equity, and inclusion practices.

5. Supporting documentation to demonstrate that expenses are allowable, allocable, reasonable, and necessary under 2 CFR part 200 and in compliance with the grant's NOFO, award terms, and applicable federal regulations.

O. Immigration Conditions

A recipient under this funding opportunity must comply with the FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025), with the exception Paragraph C.IX (Communication and Cooperation with the Department of Homeland Security and Immigration Officials) and paragraph C.XVII(2)(a)(iii) (Anti-Discrimination Grant Award Certification regarding immigration). Paragraphs C.IX and C.XVII(2)(a)(iii) do not apply to any federal award under this funding opportunity. The FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025) are available at www.dhs.gov/publication/dhs-standard-terms-and-conditions.

10. Other Information

A. Period of Performance Extension

Extensions to the period of performance are allowed.

Recipients should consult with their FEMA point of contact for requirements related to a performance period extension.

B. Other Information

a. *Environmental Planning and Historic Preservation (EHP) Compliance*

FEMA is required to consider effects of its actions on the environment and historic properties to ensure that activities, grants and programs funded by FEMA, comply with federal EHP laws, Executive Orders, regulations, and policies.

Recipients and subrecipients proposing projects with the potential to impact the environment or cultural resources, such as the modification or renovation of existing buildings, structures, and facilities, and/or new construction and/or replacement of buildings, structures, and facilities, must participate in the FEMA EHP review process. This includes conducting early engagement to help identify EHP resources, such as threatened or endangered species and, historic properties, submitting a detailed project description with supporting documentation to determine whether the proposed project has the potential to impact EHP resources; and, identifying mitigation measures and/or alternative courses of action that may lessen impacts to those resources.

FEMA is sometimes required to consult with other regulatory agencies and the public in order to complete the review process. Federal law requires EHP review to be completed before federal funds are released to carry out proposed projects. FEMA may not be able to fund projects that are not in compliance with applicable EHP laws, Executive Orders, regulations, and policies. FEMA may recommend mitigation measures and/or alternative courses of action to lessen impacts to EHP resources and bring the project into EHP compliance.

EHP guidance is found at Environmental Planning and Historic Preservation. The site contains links to documents identifying agency EHP responsibilities and program requirements, such as implementation of the National Environmental Policy Act and other EHP laws, regulations, and Executive Orders. DHS and FEMA EHP policy is also found in the EHP Directive & Instruction.

All FEMA actions, including grants, must comply with National Flood Insurance Program (NFIP) criteria or any more restrictive federal, state, or local floodplain management standards or building code (44 C.F.R. § 9.11(d)(6)). For actions located within or that may affect a floodplain or wetland, the following alternatives must be considered: a) no action; b) alternative locations; and c) alternative actions, including alternative actions that use natural features or nature-based solutions. Where possible, natural features and nature-based solutions shall be used. If not practicable as an alternative on their own, natural features and nature-based solutions may be incorporated into actions as minimization measures.

The GPD EHP screening form is located at https://www.fema.gov/sites/default/files/documents/fema_ehp-screening_form_ff-207-fy-21-100_5-26-2021.pdf.

b. *Procurement Integrity*

When purchasing under a FEMA award, recipients and subrecipients must comply with the federal procurement standards in 2 C.F.R. §§ 200.317-200.327.. To assist with determining whether an action is a procurement or instead a subaward, please consult 2 C.F.R. § 200.331. For detailed guidance on the federal procurement standards, recipients and subrecipients should refer to various materials issued by FEMA's Procurement Disaster Assistance Team (PDAT).

Additional resources, including an upcoming trainings schedule can be found on the PDAT Website: https://www.fema.gov/grants/procurement.

Under 2 C.F.R. § 200.317 when procuring property and services under a federal award, States (including territories) and Tribal Nations, must follow the same policies and procedures they use for procurements from their non-federal funds; additionally, states and Tribal Nations must now follow 2 CFR §200.322, regarding domestic preferences for Procurements and 2 CFR§ 200.327 regarding required contract provisions.

Local government and nonprofit recipients or subrecipients must have and use their own documented procurement procedures that reflect applicable State, Local, Tribal, and Territorial (SLTT) laws and regulations, provided that the procurements conform to applicable federal law and the standards identified in 2 C.F.R. Part 200.

1. Important Changes to Procurement Standards in 2 C.F.R. Part 200

On April 22, 2024, OMB updated various parts of Title 2 of the Code of Federal Regulations, among them the procurement standards. These revisions apply to all FEMA awards with a federal award date or disaster declaration date on or after October 1, 2024, unless specified otherwise. The changes include updates to the federal procurement standards, which govern how FEMA award recipients and subrecipients must purchase under a FEMA award.

More information on OMB's revisions to the federal procurement standards can be found in Purchasing Under a FEMA Award: 2024 OMB Revisions Fact Sheet.

2. Competition and Conflicts of Interest

2 CFR §200.319(b) , applicable to local government and nonprofit recipients or subrecipients, requires that contractors that develop or draft specifications, requirements statements of work, or invitations for bids or requests for proposals must be excluded from competing for such procurements. FEMA considers these actions to be an organizational conflict of interest and interprets this restriction as applying to contractors that help a recipient or subrecipient develop its grant application, project plans, or project budget. This prohibition also applies to the use of former employees to manage the grant or carry out a contract when those former employees worked on such activities while they were employees of the recipient or subrecipient.

Under this prohibition, unless the recipient or subrecipient solicits for and awards a contract covering both development and execution of specifications (or similar elements as described above), and this contract was procured in compliance with 2 C.F.R. § § 200.317-200.327, federal funds cannot be used to pay a contractor to carry out the work if that contractor also worked on the development of those specifications. This rule applies to all contracts funded with federal grant funds, including pre-award costs, such as grant writer fees, as well as post- award costs, such as grant management fees.

In addition to organizational conflicts of interest, situations considered to be restrictive of competition include, but are not limited to:

- Placing unreasonable requirements on firms for them to qualify to do business;
- Requiring unnecessary experience and excessive bonding;
- Noncompetitive pricing practices between firms or between affiliated companies;
- Noncompetitive contracts to consultants that are on retainer contracts;
- Specifying only a "brand name" product instead of allowing "an equal" product to be offered and describing the performance or other relevant requirements of the procurement; and
- Any arbitrary action in the procurement process.

Under 2 C.F.R§ 200.318(i), local government and nonprofit recipients or subrecipients are required to maintain written standards of conduct covering conflicts of interest and governing the actions of their employees engaged in the selection, award, and administration of contracts. **No employee, officer, or agent may participate in the selection, award, or administration of a contract supported by a federal award if he or she has a real or apparent conflict of interest. Such conflicts of interest would arise when the employee, officer or agent, any member of his or her immediate family, his or her partner, or an organization that employs or is about to employ any of the parties indicated herein, has a financial or other interest in or a tangible personal benefit from a firm considered for a contract. The officers, employees, and agents of the recipient or subrecipient may neither solicit nor accept gratuities, favors, or anything of monetary value from contractors or parties to subcontracts. However, the recipient or subrecipient may set standards for situations in which the financial interest is not substantial, or the gift is an unsolicited item of nominal value. The recipient's or subrecipient's standards of conduct must provide for disciplinary actions to be applied for violations of such standards by officers, employees, or agents.**

Under 2 C.F.R. 200.318(c)(2), if the local government and nonprofit recipient or subrecipient has a parent, affiliate, or subsidiary organization that is not a SLTT government, the recipient or subrecipient must also maintain written standards of conduct covering organizational conflicts of interest. Organizational conflict of interest means that because of a relationship with a parent company, affiliate, or subsidiary organization, the recipient or subrecipient is unable or appears to be unable to be impartial in conducting a procurement action involving a related organization. The recipient or subrecipient must disclose in writing any potential conflicts of interest to FEMA or the pass-through entity in accordance with applicable FEMA policy.

3. Supply Schedules and Purchasing Programs

Generally, a recipient or subrecipient may seek to procure goods or services from a federal supply schedule, state supply schedule, or group purchasing agreement.

Information about GSA programs for states, Tribal Nations, and local governments, and their instrumentalities, can be found at Purchasing Resources and Support for State and Local Governments.pdf

4. Procurement Documentation

Per 2 C.F. R§ 200.318(i), local government and nonprofit recipients or subrecipients are required to maintain and retain records sufficient to detail the history of procurement covering at least the rationale for the procurement method, selection of contract type, contractor selection or rejection, and the basis for the contract price. States and Indian Tribes are reminded that in order for any cost to be allowable, it must be adequately documented per 2 CFR §200.403(g).

Examples of the types of documents that would cover this information include but are not limited to:

- Solicitation documentation, such as requests for quotes, invitations for bids, or requests for proposals;
- Responses to solicitations, such as quotes, bids, or proposals;
- Pre-solicitation independent cost estimates and post-solicitation cost/price analyses on file for review by federal personnel, if applicable;
- Contract documents and amendments, including required contract provisions; and
- Other documents required by federal regulations applicable at the time a grant is awarded to a recipient.

c. *Financial Assistance Programs for Infrastructure*

1. Build America, Buy America Act
Not applicable

d. *Mandatory Disclosures*

The non-Federal entity or applicant for a federal award must disclose, in a timely manner, in writing to the federal awarding agency or pass-through entity all violations of federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award, 2 CFR § 200.113 .

e. *Adaptive Support*

Pursuant to Section 504, of the Rehabilitation Act of 1973 , recipients of FEMA financial assistance must ensure that their programs and activities do not discriminate against qualified individuals with disabilities.

f. *Record Retention*

1. Record Retention Period

Financial records, supporting documents, statistical records, and all other non-Federal entity records pertinent to a federal award generally must be maintained for at least three years from the date the final FFR is submitted. *See* 2 C.F.R. §200.334. Further, if the recipient does not submit a final FFR and the award is administratively closed, FEMA uses the date of administrative closeout as the start of the general record retention period.

The record retention period **may be longer than three years or have a different start date** in certain cases.

2. Types of Records to Retain

FEMA requires that recipients and subrecipients maintain the following documentation for federally funded purchases:

- Specifications
- Solicitations
- Competitive quotes or proposals
- Basis for selection decisions
- Purchase orders
- Contracts
- Invoices
- Cancelled checks

g. *Actions to Address Noncompliance*

Non-federal entities receiving financial assistance funding from FEMA are required to comply with requirements in the terms and conditions of their awards or subawards, including the terms set forth in applicable federal statutes, regulations, NOFOs, and policies. Throughout the award lifecycle or even after an award has been closed, FEMA or the pass-through entity may discover potential or actual noncompliance on the part of a recipient or subrecipient.

In the case of any potential or actual noncompliance, FEMA may place special conditions on an award per 2 C.F.R.§ 200.208 and 2 C.F.R.§ 200.339. FEMA may place a hold on funds until the matter is corrected, or additional information is provided per 2 C.F.R.§ 200.339. or it may do both. Similar remedies for noncompliance with certain federal civil rights laws are authorized pursuant to 2 C.F.R.44 CFR Part 7 and 2 C.F.R. 44 Part 19 or other applicable regulations.

If the noncompliance is not able to be corrected by imposing additional conditions or the recipient or subrecipient refuses to correct the matter, FEMA may take other remedies allowed under 2 C.F.R.§ 200.339.

i. *Audits*

FEMA grant recipients are subject to audit oversight from multiple entities including the DHS OIG, the GAO, the pass-through entity, or independent auditing firms for single audits, and may cover activities and costs incurred under the award. Auditing agencies such as the DHS OIG, the GAO, and the pass-through entity (if applicable), and FEMA in its oversight capacity, must have access to records pertaining to the FEMA award.

j. Appendices

Appendix A: Program Guidelines and Application Content Requirements

Overview.
Over the last several years our nation has witnessed an exponential rise in Nation State and organized crime threat vectors and cyber-attacks with disruptive and destructive physical consequences. Industrial control systems and other supporting information technology which power energy, water, communications, and other critical infrastructure sectors are becoming increasingly interdependent and attractive as targets.

Needs Analysis.
The NCPC's training proposal/statement of work must identify and explain preparedness gaps that could be addressed through cybersecurity training development and delivery that are distinct from other national training programs and FEMA courses. NCPC partners will use NTED's Unified Training Needs Assessment (UTNA) process to verify that training solutions to be developed, or to be sustained target the need, align with the FEMA mission, focused on performance-level and planning and management level curricula, are not duplicative, and are cost effective in terms of content, modality, and delivery.

Target Audience.
Cybersecurity training must empower technical and non-technical personnel in key roles including cybersecurity and information technology professionals, leadership and organizational decision makers, SLTT emergency responders and end users.

Standards.
The status of Executive Orders and other standards are fluid. Some items included on this list may no longer appear on government websites but are still promulgated in the Federal Register at this time. Proposed training must be consistent with the guidelines found in the following:

- Executive Order 14144: Strengthening and Promoting Innovation in the Nation's Cybersecurity January 17, 2025. Federal Register :: Strengthening and Promoting Innovation in the Nation's Cybersecurity

- Executive Order 14028: Improving the Nation's Cybersecurity. Signed by President Biden May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

- Executive Order 13636: Improving Critical Infrastructure Cybersecurity. Signed by President Obama February 12, 2013. Additional information can be found at https://www.Federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

- Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Signed by President Trump May 11, 2017. Additional information

can be found at www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

- DHS's Critical Infrastructure Cyber Community C³ Voluntary Program also provides resources to support critical infrastructure owners and operators in the adoption of the Framework to manage cyber risk more effectively. It was launched in February 2014 to support Executive Order 13636. Additional information on the C³ Program can be found at https://www.cisa.gov/sites/default/files/c3vp/Cyber_Communication_Resources.pdf *;*

- The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 to better manage cybersecurity risk. This document was released February 26, 2024 and is available at https://www.nist.gov/cyberframework;

- The National Institute of Standards and Technology (NIST) NICE Framework Components v1.0.0 released in March 2024. This document is available at https://niccs.cisa.gov/workforce-development/nice-framework

- The Nationwide Cyber Security Review (NCSR) findings and recommendations. The NCSR identifies the level of maturity and risk awareness of state and local government information. This document is available at https://cisecurity.org/ms-isac/services/ncsr

- The Comprehensive National Cybersecurity Initiative (CNCI) consists of initiatives and goals designed to help secure the United States in cyberspace. https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

- IT Sector Baseline Risk Assessment The ITSRA identifies and prioritizes national-level risks to critical functions delivered and maintained by the IT Sector and relied on by all critical infrastructure sectors. https://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf

- Office of Management and Budget Guidance on FISMA M-22-05 provides current Administration information security priorities, FY 2021-2022 Federal Information Security Management Act (FISMA) and Privacy Management reporting guidance and deadlines, and policy guidelines to improve Federal information security posture. FISMA report Final - FY 2022.pdf

- Executive Order 14141: Advancing United States Leadership in Artificial Intelligence Infrastructure. Signed by President Biden January 17, 2025. Additional information can be found at Federal Register: Advancing United States Leadership in Artificial Intelligence Infrastructure

- NIST Special Publication 800-series comprises guidelines, recommendations, and technical specifications for cybersecurity and privacy. www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

- U.S. Election Assistance Commission's Election Supporting Technology Evaluation Program (ESTEP). https://www.eac.gov/election-technology/estep-program

- U.S. Customs and Border Protection Cybersecurity Strategy. www.cbp.gov/sites/default/files/assets/documents/2016-Jul/cbp-cyberstrategy-20160720.pdf

- Higher Education Community Vendor Assessment Toolkit is a questionnaire framework to measure vendor risk. https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit

- National Security Agency and Cybersecurity and Infrastructure Security Agency's Mitigate Risks from Managed Service Providers in Cloud Environments. https://media.defense.gov/2024/Mar/07/2003407859/-1/-1/0/CSI-CloudTop10-Managed-Service-Providers.PDF

- CISA Cloud Security Technical Reference Architecture. Provides recommended approaches to cloud migration and data protection for agency data collection and reporting that leverages Cloud Security Posture Management (CSPM). This technical reference architecture also informs agencies of the advantages and inherent risks of adopting cloud-based services as agencies implement to zero trust architectures. Cloud Security Technical Reference Architecture v.2

- CISA's Binding Operational Directive 25-01: Implementing Secure Practices for Cloud Services. This Directive applies to all production or operational cloud tenants (operating in or as federal information systems) with an associated and finalized Secure Cloud Business Applications (SCuBA) Secure Configuration Baselines published by CISA. Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 25-01: Implementing Secure Practices for Cloud Services

- NIST Cloud Computing Security Reference Architecture (SP 500-292). Outlines a cloud security architecture that defines the roles, services, and activities of key cloud actors, including consumers, providers, auditors, brokers, and carriers. NIST Cloud Computing Security Reference Architecture (SP 500-292)

- NIST Guidelines on Security and Privacy in Public Cloud Computing (SP 800-144). It emphasizes the shared responsibility model. NIST Special Publication 800-144

- NIST Zero Trust Architecture (SP 800-207). Provides a technical reference architecture for zero trust. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

- NIST A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments (SP 800-207A). Explains how organizations can implement zero trust access control for cloud-native applications consistent with the concepts and principles outlined in NIST Special Publication (SP) 800-207, Zero Trust Architecture. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207A.pdf

- CISA Zero Trust Maturity Model. Provides an approach to achieve continued modernization efforts related to zero trust within a rapidly evolving environment and technology landscape. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

- Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA) - Port Facility Cybersecurity Risks: https://www.cisa.gov/sites/default/files/publications/port-facility-cybersecurity-risks-infographic_508.pdf

- National Security Agency (NSA), ODNI, and DHS/CISA - Developers Recommended Practices Guide for Securing the Software Supply Chain: https://media.defense.gov/2022/Sep/01/2003068942/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF

- Federal Register - Entry on the Entity List (Nuctech): https://www.federalregister.gov/documents/2020/12/22/2020-28031/addition-of-entities-to-the-entity-list-revision-of-entry-on-the-entity-list-and-removal-of-entities

- Federal Bureau of Investigation (FBI) - Worldwide Threats to the Homeland: https://www.fbi.gov/news/testimony/worldwide-threats-to-the-homeland-111522

- ODNI - 2023 Annual Threat Assessment of the U.S. Intelligence Community: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

Adult Learning Approach.

NCPC training programs will use an adult learning approach across of variety of modalities and delivery methods including classroom instruction, virtual training, learning through workshops and seminars, interactive web-based and computer-based training. Adult learning theory includes the following key components outlining the general ways in which adults perceive learning and how they prefer to train: Self-Concept, Adult Learner Experience, Readiness to Learn, Orientation of Learning, and Motivation to Learn.

Instructional Systems Design (ISD) Expertise.
NCPC partners must have staff members qualified in the field of ISD whose primary responsibilities are to design, develop, and review instructional content for web-based and/or instructor-led courseware.

Non-Duplication of Existing Training Programs.
NCPC-developed training must not duplicate training provided by Federal, state, local, tribal, or territorial departments and agencies, or other training providers.

Recertification of Existing Training Programs.
NCPC developed training must submit to recertification of courses every three years to maintain relevance, accuracy, and effectiveness.

Course Mapping.
NCPC partners will use NTED's course mapping process to determine appropriate course complexity, learning levels, and alignment with Mission Areas and Core Capabilities.

Application Content. The NCPC application must include the following:

Executive Summary. The NCPC applicant must provide, in the order presented below, an executive summary that includes the following data and information as appropriate using the below template:

EXECUTIVE SUMMARY TEMPLATE

Organization Name: [Insert Org Name]
Submission Date: [mo/day/yr]

Summarize, in the order presented below, the following information and data as appropriate.

1. **Total Number of NTED Certified Courses: [Insert Number]**
2. **Certified Course List and Performance Targets [Fill in table, below]**

Course Number	Course Title	Most Recent Certification Date	Average Cost Per Student (by course)	Anticipated Student Throughput for this PoP	Proposed Number of Deliveries for this PoP

3. Proposed New Courses and Overviews [Fill in table, below]

Proposed New Courses for this Award	High Level Rationale for Proposed New Course	Average Cost Per Student (by course)	Anticipated Student Throughput for this PoP	Proposed number of deliveries for this PoP
Course: [Course Title and Description]				

Program Narrative, Part 1. Provide detailed explanations for the following:

- Program alignment with the National Preparedness Goal, National Preparedness System, National Incident Management System, National Planning Frameworks, Mission Areas, and Core Capabilities.
- Description of program management structures to illustrate how the program is organized and managed within the NCPC. The NCPC must provide an organizational chart and describe how the organization will support the program.
- A detailed program schedule to reflect the program life cycle with phases, deliverables, and outcomes arranged and explained. Include specific course information and timelines for all upcoming NTED course recertifications.
- A process for identifying lessons learned and best practices for ongoing FEMA and DHS efforts.

Program Narrative, Part 2 (Training Objectives). The NCPC must describe their planned approach to design, develop, implement, and evaluate training. Training courses shall be developed and delivered as instructor-led training, designed at the performance or management level, and align to the following objectives:

Enable SLTT and applicable community members to identify, detect, and respond to cyber threats, incidents and attacks from well-resourced adversaries (e.g., nation-states, organized cyber-crime). Training should:

- Provide SLTT community organizations with a comprehensive understanding of the threat posed by organized, highly funded and sophisticated threat actors that may be motivated by political or economic causes such as nation-states or organized cyber-

crime intent on disrupting critical infrastructure systems or accessing sensitive or private data. Cybersecurity threats to the SLTT community should be considered in both an intra-jurisdictional and extra-jurisdictional context with respect to authorities and mission critical impact.

- Present methods of identifying potential vulnerabilities or threat activity based on observed data and known attack vectors through behavioral analysis, pattern identification, system activity thresholds, endpoint analysis and network traffic analysis.
- Instruct SLTT organizations on methods to establish and operate continuous monitoring and detection systems and processes that establish baseline network system patterns and identify statistical outliers and anomalies that could indicate a cyber incident or attack.
- Address the need to monitor and analyze endpoint activities to detect and respond to threats and examine network traffic for signs of malicious activity or data exfiltration.
- Educate SLTT organizations on analytical methods and models to improve monitoring and detection abilities.
- Enhance SLTT community organizations' ability to recognize adversary information warfare capabilities and identify tactics, techniques, and procedures employed by well-resourced adversaries. Train community to apply threat intelligence to enhance detection and response capabilities.
- Educate the SLTT community in threat hunting, hunt hypotheses development, and deliberate usage of previously described methods to locate current and undiscovered threat activity on the network.
- Develop SLTT community organizations' ability to apply advanced information sharing mechanisms and techniques to collectively improve cybersecurity detection and response.
- Assess the need for digital forensics activities to include malware analysis, and utilization of Artificial Intelligence/Machine Learning (AI/ML) algorithms to analyze large datasets quickly and accurately to identify patterns and anomalies. Digital forensics capacity should cover traditional/legacy information technology environments, as well as cloud, hybrid, multi-tenant, Internet of Things (IoT) and mobile devices.

Enable SLTT and applicable community members to identify, maintain, sustain, protect and recover logistics capabilities in transportation (Highway/Roadway, Mass Transit, Railway, Aviation, and Maritime) when information systems are degraded during cyber incidents. Training should:

- Provide focused cybersecurity education for specific transportation sectors *(Highway/Roadway, Mass Transit, Railway, Aviation, Maritime)* or integrated combinations of multiple sectors, as applicable.
- Enable SLTT and the applicable community to address unique problems and issues related to cybersecurity in logistics systems utilizing autonomous vehicles and

drones, particularly in roadway, aviation, and maritime verticals during normal and degraded conditions.

- Educate SLTT communities on the importance of cybersecurity for logistics in emergency management and community resilience and how incidents in the private sector may impact the public sector vice versa.
- Develop SLTT community logistics maintenance and sustainment capabilities for use during cyber incidents.
- Instruct SLTT community members in the role of technology in sustaining logistics (e.g., Transportation Management Systems, GPS tracking), as well as cybersecurity measures for protecting transportation logistics.
- Demonstrate strategies for continuity of operations when information systems are compromised, and disaster recovery challenges within logistics capabilities and systems.
- Enable information sharing and coordination between federal, state, and local agencies and communities during recovery efforts.
- Provide for organizational incident response planning, organizing, equipping, training and exercise (POETE) in preparation for cyber and/or all-hazard incidents.
- Educate SLTT community members in building resilient logistics networks through Community engagement and collaboration with private sector, nonprofits, and community organizations.
- Utilize real-world examples of logistics challenges and solutions during cyber incidents to demonstrate methods for resiliency.
- Assess emerging technologies and innovations in logistics, along with future cybersecurity threats in logistics and how to prepare for them.

Work Breakdown Structure. The NCPC will provide a work breakdown structure (WBS) as part of the application. A WBS is a task-oriented schematic of activities that organizes, defines, and graphically displays the total work to achieve the final objectives of a project.
The WBS applies a system for subdividing a project into manageable work packages, components, or elements to provide a common framework for scope/cost/schedule communications, allocation of responsibility, risk management, performance-based evaluations, and a quality control plan. The WBS establishes deliverables arranged on an anticipated timeline. Each descending level represents an increasingly detailed definition of the project objective. Components of the WBS include, but are not limited to, the following:

- A risk management plan describing the approach for identifying and managing risks, and identifying known or postulated events or factors that could prevent a recipient from meeting program objectives (cost, schedule, scope, performance, or quality);
- A performance-based evaluation plan, including program performance measures that will assess the attainment of goals, objectives, outcomes, and which details a data collection plan including the analysis of data; and

- A quality control plan for the development and delivery of programs and courses.

Equipment Plan. The NCPC must provide an equipment-purchasing plan for proposed equipment purchases that are required to support the program. At a minimum, the plan must detail planned equipment purchases, why they are necessary, and the costs of the equipment.

Detailed Budget. The NCPC must provide a detailed budget by task and a summary budget aggregating task costs into the categories of personnel, fringe benefits, travel, equipment, supplies, consultants/contracts, other costs, indirect costs, and the total budget. Submit the detailed budget with the grant application as a file attachment within FEMA GO. The budget must be complete, reasonable, and cost-effective in relation to the proposed project. The budget should provide the basis of computation of all project-related costs, any appropriate narrative, and a detailed justification of M&A costs. Budget information must also address the following:

- **PERSONNEL.** The NCPC must indicate the total projected salary and wages for all project personnel. Compensation paid for employees engaged in activities must be consistent with that paid for similar work within the NCPC organization.
- **TRAVEL.** The NCPC must provide the total projected cost for travel. The NCPC should determine costs by the projected number of trips multiplied by the number of people traveling multiplied by an average cost for travel and per diem (airfare, lodging, meals). Separate travel for development of training and delivery of training in the detailed budget but include all travel costs as a single total in the summary budget. Detail travel performed at the request of NTED under travel for development of training.
- **EQUIPMENT.** The NCPC must provide the total projected cost for non-expendable items. Non-expendable equipment is tangible property having a useful life of more than one year and an acquisition cost of $5,000 or more per unit. The NCPC may use the organization's own capitalization policy and threshold amount for classification of equipment. Expendable items should be included in the "Supplies" category. The NCPC should analyze the cost benefits of purchasing versus leasing equipment, especially high-cost items, and those subject to rapid technical advances. List rented or leased equipment costs in the "Contracts" category. Identify and explain equipment purchases.
- **SUPPLIES.** The NCPC must provide the total projected cost of supplies (e.g., office supplies, postage, training materials, copying paper, and other expendable items, such as books and hand-held tape-recording devices). The organization's own capitalization policy and threshold amount for classification of supplies may be used. Generally, supplies include any materials that are expendable or consumed during the project.
- **CONSULTANTS/CONTRACTS.** The NCPC must provide the total projected cost of consultants and contracts. Identify and justify the type of consultant/contract.
- **OTHER COSTS.** The NCPC must provide a total projected cost of miscellaneous items (e.g., rent, reproduction, telephone, janitorial or security services, and investigative or confidential funds).

INDIRECT COSTS. A copy of an active indirect cost rate agreement must be included in the detailed budget as required for all NCPC applicants. FEMA will evaluate indirect costs as part of the application for Federal funds to determine if allowable and reasonable.