The Department of Homeland Security (DHS)
Notice of Funding Opportunity (NOFO)
Cybersecurity Workforce Development and Training for Underserved Communities

All entities wishing to do business with the federal government must have a unique entity identifier (UEI). The UEI number is issued by the SAM system. Requesting a UEI (Sam.gov information can be found at: https://sam.gov/content/entity-registration.

All entities wishing to do business with the federal government must have a unique entity identifier (UEI). The UEI number is issued by the SAM system. Requesting a UEI (Sam.gov information can be found at: https://sam.gov/content/entity-registration.

Grants.gov registration information can be found at:
https://www.grants.gov/web/grants/register.html.

1. **Planned UEI Updates in Grant Application Forms**

   On April 4, 2022, the Data Universal Numbering System (DUNS) Number was replaced by a new, non-proprietary identifier requested in, and assigned by, the System for Award Management (SAM.gov). This new identifier is the Unique Entity Identifier (UEI). Additional Information can be found on Grants.gov:
   https://www.grants.gov/web/grants/forms/planned-uei-updates.html

A. Program Description

1. **Issued By**
   U.S. Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA)

2. **Assistance Listing Number**
   97.127

3. **Assistance Listing Title**
   Cybersecurity Education and Training

4. **Funding Opportunity Title**
   Cybersecurity Workforce Development and Training for Underserved Communities

5. **Funding Opportunity Number**
   DHS-23-CISA-127-CWDT-0001

6. **Authorizing Authority for Program**
   Homeland Security Act of 2002, Pub. L. No. 107-296, § 102(b)(2) (codified as amended (6 U.S.C. § 112(b)(2)).

7. **Appropriation Authority for Program**
   Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, Division F – Department of Homeland Security Appropriations Act, 2023, Title III Protection, Preparedness, Response, and Recovery, Cybersecurity and Infrastructure Security Agency

8. **Announcement Type**
   Initial

9. Program Overview, Allowable Activities, Objectives, and Priorities

a. Program Overview

The nature of the cybersecurity threat to America is growing, and our nation's cyber adversaries move with speed and stealth. In alignment with the Department of Homeland Security's Strategic Plan for Fiscal Years 2020-2024, it is imperative to not only secure cyberspace and critical infrastructure, but we must also strengthen our preparedness and resilience, including ensuring that we have a skilled workforce to defend our networks. We therefore must ensure equal access to professional development opportunities to fill cyber vacancies across our country and to prevent future shortages that threaten our ability to compete. Maintaining a highly skilled, diverse, and engaged workforce is critical to ensuring the public and private sectors can protect the nation's cyberspace and support the accomplishment of the Department's mission, which relies on dedicated personnel who go above and beyond to keep Americans safe from harm. However, per cyberseek.org, there were over 755,000 cybersecurity job openings nationwide in 2022 – a shortage that puts our nation at a dangerous technological disadvantage and an increased risk of malicious cyber activity.

The Cybersecurity and Infrastructure Security Agency (CISA), Cyber Defense Education & Training (CDET) team is committed to strengthening the nation's federal and national cybersecurity workforce through standardizing roles and helping to ensure we have well-trained cybersecurity professionals today as well as a strong pipeline of future cybersecurity leaders tomorrow.

Strengthening our cybersecurity workforce requires diverse perspectives from communities that represent America. Increasing the number of cybersecurity professionals within underserved communities is key to the success of our nation. These professionals are critical in both private industry and the government for the security of the nation.

Furthermore, the retention of individuals with these skills is an important element in the development of our Nation's cybersecurity workforce. As the nation responds to ongoing rapid technological changes and advances, the non-traditional workforce system plays an essential part in providing a skilled workforce to fill critical shortages. Non-traditional technical training providers (NTTPs) are entities that actively provide cybersecurity training, internships, apprenticeships, and/or other work-based learning approaches to meet the dynamic needs the cybersecurity workplace. To remain competitive, our nation will need to reimagine how it educates and trains entry-level cyber professionals.

CDET seeks to award a cooperative agreement titled "*Cybersecurity Workforce Development and Training for Underserved Communities*" in fiscal year 2023. The activities contemplated in this agreement advance CISA's mission as defined in authorities within the Homeland Security Act of 2002, as amended by the Cybersecurity and Infrastructure Security Agency Act of 2018, specifically as it relates to providing shared situational awareness to enable real-time, integrated, and

operational actions across the Federal Government and non-Federal entities to address cybersecurity risks and incidents.

The activities contemplated in the agreement broadly support the Department of Homeland Security mission to safeguard the American people, through establishing a qualified cadre of cybersecurity professionals. Additionally, this agreement directly aligns to the CISA's Strategic Plan 2023-2024; by providing federal funding to NTTPs to develop and execute cybersecurity training and assist trainees in securing internships, apprenticeships, and/or employment to support the dynamic needs of the cybersecurity workplace. The NTTPs efforts must be directed primarily to members of underserved[1] communities as an opportunity to pursue a career that may otherwise be unfamiliar or unattainable. This cooperative agreement seeks to fund applicants to develop and execute a scalable program that can respond to the nation's cyber eco-system challenges.

This cooperative agreement also seeks to leverage the unrealized cybersecurity talent of underserved communities through established or emerging NTTPs that create or enhance existing entry-level training and apprenticeship and programs. Additionally, to optimize and expand existing cybersecurity training and placement programs, the development and implementation of a comprehensive cybersecurity pathways retention strategy to address enrollment-to-placement engagement, is needed. Applicants will work collaboratively to align resources in response to workforce demand and to offer innovative job training solutions that generate positive outcomes and results.

The intent of this cooperative agreement is to fund a program which will enable NTTPs to provide training to a target audience of underserved individuals that are at least 17 years old that, as a result of the training, will gain the skills and competencies required to secure entry-level skilled cybersecurity jobs. Underserved communities include Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality that have been denied opportunities to receive cyber-related education and who are seeking full-time employment into entry-level skilled cybersecurity positions.

* Per Executive Order 13985: "The term "underserved communities" refers to populations sharing a particular characteristic, as well as geographic communities, that have been systematically denied a full opportunity to participate in aspects of economic, social, and civic life..."

b. Objectives

All applicants should clearly state how the following objectives would be addressed in their application.

i. Implement an engaging training hub (virtual, in person, or a hybrid combination) covering both national and regional cybersecurity challenges to deliver cybersecurity training to underserved communities and connect participants and employers in one or more CISA regions.

ii. Implement an apprenticeship and/or placement program for entry-level cybersecurity professionals that's supported by affiliations with cybersecurity entities who may support program enrollees and/or graduates.

iii. Decrease the cybersecurity workforce shortage and equity gap by placing NTTP program graduates into full-time, entry-level cybersecurity jobs.

c. Program Priorities

a. Program participants are selected from underserved communities

b. Program participants complete a NICE Framework-mapped cybersecurity training curriculum

c. Program graduates are competitive candidates for apprenticeships and/or entry-level cybersecurity jobs

d. Applicant recruits participants and employers in one or more CISA regions

e. Applicant provides a sharable NICE Framework-mapped training curriculum

f. Applicant submits proof of concept with recommendations to replicate on larger scale

d. Allowable Activities

The Cybersecurity Workforce Development and Training Program for Underserved Communities funding will ensure equal access to professional development opportunities to fill cyber vacancies in the USA by strengthening the nation's federal and national cybersecurity workforce through diverse perspectives from underserved communities. Successful applicants will design their approach from both (1) a strategic level, such as describing the planned activities for devising a cybersecurity training, placement, and sustainability strategy; and (2) an operational level, such as plans for implementation of the proposed strategy including development of a placement pipeline and deployment of the training activities to underserved individuals. Applicants must propose projects that comprise the following activities:

i. Draft for CISA's review and, upon approval, execute a cybersecurity training, placement, and sustainability strategy (herein referred to as a Cybersecurity Pathways Retention Strategy (CPRS) for underserved communities and a detailed implementation schedule, including:

1) Develop a new or leverage an existing system for reviewing and collecting data and monitor results to assess the 3-year program performance.

2) Create a new or leverage an existing infrastructure to successfully sustain the program components and partnerships after the life of the cooperative agreement.

ii. Create an engaging, effective, and inclusive training hub (virtual, in person or a hybrid of both) in one or more CISA regions, where:

1) Individuals from underserved communities have access to high-quality training options (such as computer-based and/or work-based) to prepare them for successful placement into entry-level cybersecurity occupations.

2) Training participants are introduced to cybersecurity career options aligned to the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework) to include sample job roles and responsibilities.

3) Training participants are introduced to professionals who represent the cybersecurity career field.

iii. Career Pathways: Career pathway strategies shall integrate formal occupational skills training with employer-validated work readiness and may include pre-apprenticeships and/or apprenticeships as a precursor to obtaining full-time, entry-level cybersecurity employment. The clear sequence of coursework and hands-on/real-world professional training should outline the necessary steps required for training participants to gain demonstratable and marketable skills that will make them a competitive job candidate for various entry-level cybersecurity occupations.

iv. Support Services: Projects funded under this cooperative agreement will provide a range of training and support services that lead to entry-level skilled cybersecurity jobs. An innovative mix of services shall include assessment, coaching, counseling, and occupational skills training that ultimately leads to job placement. All projects must incorporate a strong upfront assessment component that allows for a customization of training and support to effectively meet the needs of the underserved program participants. This could include the use of customized online assessment tools.

v. Establish/expand the organization's professional network of cybersecurity partners/affiliates who may provide insight on current workforce recruitment efforts that help shape the development of the training and placement program. These networks will support participants of the cybersecurity training program by offering an apprenticeship and/or full-time employment to program graduates. Employers will be introduced to the depth and scope of the training and placement program with a goal to aid underserved individuals in achieving their cybersecurity career goals while simultaneously advancing their own internal recruiting and hiring efforts.

vi. Applicants must include robust, comprehensive, and customized learning strategies when developing the training program which must be aligned with the NICE Framework. Applicants shall propose one or more of the following strategies that best meet the needs of both program graduates and potential employers while allowing for flexibility in program delivery.

1) Customized Training: Cohort-based customized training is designed to meet the specific requirements of an employer or group of employers with the commitment that the employer(s) hire an individual upon successful completion of the training.
2) Pre-Apprenticeship Programs: A pre-apprenticeship program is a bridge to career opportunities for underprepared learners that must link directly to existing apprenticeship programs and provides instruction, preparation, and support as part of a career pathway. This endeavor provides individuals an opportunity to explore a variety of cybersecurity careers and interact with industry professionals. Pre-apprenticeship programs funded through this cooperative agreement are allowable only when participants are selected for an apprenticeship program(s) during the period of performance.

3) Registered Apprenticeship Programs (RAP): RAPs (29 CFR Part 29, Subpart A, and 29 CFR Part 30) combine an educational or instructional component with a paid work- based learning component. RAPs are registered through the DOL's Office of Apprenticeship or a DOL-recognized State Apprenticeship Agency. Registered apprentices are paid employees and receive progressive wage increases commensurate with their skill attainment throughout the training program. Registered apprentices have a 1:1 ratio with a mentor throughout their on-the-job learning. Upon successful completion of all phases of work-based learning and related-instruction components, registered apprentices receive nationally recognized certificates of completion leading to long-term career opportunities. For more information on RAPs, please visit www.apprenticeship.gov.

4) Classroom, Competency-Based and Online Training Strategies: In addition to the types of work-based training previously listed, a variety of other types of training strategies may include but are not limited to classroom occupational training; distance learning; technology-based learning; and simulation training. Accelerated and competency-based training strategies can train participants swiftly, efficiently, and effectively by providing course credit to participants for skills they have already developed and mastered. Any number of these strategies may be combined to reduce the total time required by training participants to meet credential or program requirements.

10. Performance Measures

a. Number of reciprocal arrangements with employers who place program participants in apprenticeships and/or hire program graduates as full-time employees **This refers to partners/affiliations (as evidenced by a contract, agreement, Memorandum of Understanding, Letter of Intent, etc.) with cybersecurity entities who place program enrollees and/or graduates.*

b. Number of underserved individuals enrolled in the training and placement program

c. Percent of enrolled program participants who successfully obtain an apprenticeship

d. Percent of enrolled program participants who graduate from the NTTP training program and successfully obtain full-time employment as a cybersecurity professional

See Appendix C

B. Federal Award Information

1. Available Funding for the NOFO:
$3,000,000 ($1,500,000.00 if two recipients are selected)

2. Projected number of Awards:
Minimum 2

3. Period of Performance:
Up to 36 months

4. **Projected Period of Performance Start Date(s):**
   09/30/2023

5. **Projected Period of Performance End Date(s):**
   09/29/2026

6. **Funding Instrument Type:**
   Cooperative Agreement

   DHS will exercise substantial programmatic involvement through this cooperative agreement to include review and approval of a comprehensive cybersecurity training, placement, and sustainability strategy prior to implementation of any subsequent efforts funded by this award. The Program Officer may also conduct a review of the training hub to determine compliance with the Allowable Activities outlined in Section A.9.d. before implementation may occur.

C. Eligibility Information

Non-traditional technical training providers (NTTPs) are entities that actively provide cybersecurity training, internships, apprenticeships, and/or other work-based learning approaches to meet the dynamic needs the cybersecurity workplace.

1. **Eligible Applicants**
   - **a.** Nonprofit organizations, other than institutions of higher education, with an effective ruling letter from the U.S. Internal Revenue Service granting tax exemption under Section 501(c)(3) of the Internal Revenue Code of 1986
   - **b.** Nonprofit organizations, other than institutions of higher education, without an effective ruling letter from the U.S. Internal Revenue Service granting tax exemption under Section 501(c)(3) of the Internal Revenue Code of 1986
2. **Applicant Eligibility Criteria**
   - **a. Target Community.** Applicants must have experience developing and implementing a cybersecurity training program targeting underserved communities which refers to populations sharing a particular characteristic, as well as geographic communities, that have been systematically denied a full opportunity to participate in aspects of economic, social, and civic life.
   - **b. Past Performance.** It is not a requirement to have a fully established apprenticeship and/or placement program prior to the time of applying to this cooperative agreement. Past performance in developing and implementing a cybersecurity training program is required.

3. **Other Eligibility Criteria/Restrictions**
   - **a. Required Partners**
     Applicants should forge robust partnerships to implement the cooperative agreement and to sustain activities beyond the performance period. To ensure that projects have strong and sustained employer engagement, applicants shall provide proof of existing or anticipated partnerships within the educational and professional community (i.e., after-school programs, curriculum sharing among schools, potential apprenticeship

hosts/employers, etc.). During each fiscal year throughout the period of performance, recipients are required to partner/forge partnerships with at least three employers or industry/trade associations that align with the needs of employers with entry-level skilled cybersecurity needs. An industry/trade association, also known as an industry trade group, business association, sector association, or industry body, is an organization founded and funded by businesses that operate in a specific industry. The employer partner(s) will play an important role in supporting grant success with respect to employer engagement and career pathways.

b. Optional Affiliates

We strongly encourage applicants to collaborate with other entities that can support and advance the work of bolstering the cybersecurity workforce. These include state, local, tribal, and territorial entities. Other organizations include those functioning as workforce and industry intermediaries (including entities such as workforce development entities, labor-management organizations, community-based organizations, and industry associations, which help broker local, regional, and national workforce solutions); foundations and philanthropic organizations; Federal agencies; providers of supportive and specialized services; and disability service providers.

c. Target Audience

The intent of this cooperative agreement is to fund a program which will enable NTTPs to provide in-demand training to underserved individuals who will gain the skills and competencies required to secure entry-level skilled cybersecurity jobs.

Participants of the NTTP's cybersecurity training and placement program must be at least 17 years old and, more specifically, individuals who belong to underserved communities such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality that have been denied opportunities to receive cyber-related education and who are seeking full-time employment into entry-level skilled cybersecurity positions.

4. Cost Share or Match

There is **NO** cost share requirement for this program. There is **NO** preference factor if an applicant voluntarily shares or matches costs.

D. Application and Submission Information

1. Key Dates and Times

a. Application Start Date:

05/04/2023 (open 61 days)

b. Application Submission Deadline:

07/06/2023 17:00 (GMT - 05:00) Eastern Time (US & Canada)

c. Anticipated Funding Selection Date:
No later than 09/29/2023

d. Anticipated Award Date:
No later than 09/29/2023

e. Other Key Dates

Event	Suggested Deadline for Completion
Initial Registration at SAM.gov (includes UEI issuance)	Four weeks before actual submission deadline
Obtaining a valid EIN	Four weeks before actual submission deadline
Updating SAM registration	Four weeks before actual submission deadline
Starting application in Grants.gov	Two weeks before actual submission deadline

2. Agreeing to Terms and Conditions of the Award

By applying, applicants agree to comply with the requirements of this NOFO and the terms and conditions of the award, should they receive an award.

3. Address to Request Application Package

Application forms and instructions are available at Grants.gov. To access these materials, go to http://www.grants.gov. select "Applicants" then "Apply for Grants." In order to obtain the application package, select "Download a Grant Application Package." Enter the CFDA and/or the funding opportunity number located on the cover of this NOFO, select "Download Package," and then follow the prompts to download the application package.

For a hardcopy of the full NOFO, please contact the Grants Officer by:

Email: Sean.Lilly@hq.dhs.gov
Phone: 202-601-9303

In addition, the following Telephone Device for the Deaf (TDD) and/or Federal Information Relay Service (FIRS) number available for this Notice is: 1-800-518-4726 (Grants.gov Help Desk).

Applications will be processed through the Grants.gov portal.

4. Unique entity identifier and System for Award Management (SAM)

Each applicant, unless they have a valid exception under 2 CFR § 25.110, must:

a. Be registered in SAM.gov before application submission.
b. Provide a valid unique entity identifier in its application.
c. Continue to always maintain an active SAM registration with current information during the Federal Award process.

5. **Steps Required to Submit an Application, Unique Entity Identifier, and System for Award Management (SAM)**

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

   a. Have an account with https://login.gov/
   b. Register for, update, or verify their SAM account and ensure the account is active and Employer ID Number (EIN) before submitting the application.
   c. Create a Grants.gov account.
   d. Add a profile to a Grants.gov account.
   e. Establish an Authorized Organizational Representative (AOR) in Grants.gov.
   f. Submit application in Grants.gov.
   g. Continue to maintain an active SAM registration with current information, including information on a recipient's immediate and highest-level owner and subsidiaries, as well on all predecessors that have been awarded a federal contract or grant within the last 3 years, if applicable, at all times during which it has an active federal award or an application or plan under consideration by a federal awarding agency.

   Applicants are advised that DHS may not make a federal award until the applicant has complied with all applicable SAM requirements. Therefore, an applicant's SAM registration must be active not only at the time of application, but also during the application review period and when DHS is ready to make a federal award. Further, as noted above, an applicant's or recipient's SAM registration must remain active for the duration of an active federal award. If an applicant's SAM registration is expired at the time of application, expires during application review, or expires any other time before award, DHS may determine that the applicant is not qualified to receive a federal award and use that determination as a basis for making a federal award to another applicant.

   The Standard Language for Using Grants.gov to Apply is provided to aid in fulfilling these requirements (if applicable), based off of https://www.grants.gov/web/grants/grantors/grantor-standard-language.html.

6. **Electronic Delivery**

   DHS is participating in the Grants.gov initiative to provide the grant community with a single site to find and apply for grant funding opportunities. DHS encourages or requires applicants to submit their applications online through Grants.gov, depending on the funding opportunity. For this funding opportunity, the DHS Grants and Financial Assistance Division requires applicants to submit applications through Grants.gov.

7. **How to Register to Apply through Grants.gov**

   a. Instructions: Registering in Grants.gov is a multi-step process. Read the instructions below about registering to apply for DHS funds. Applicants should read the registration instructions carefully and prepare the information requested before beginning the registration process. Reviewing and assembling the required information before beginning the registration process will alleviate last-minute searches for required information.

The registration process can take up to four weeks to complete. Therefore, registration should be done in sufficient time to ensure it does not impact your ability to meet required application submission deadlines.

Organizations must have a Unique Entity Identifier (UEI) Number with an active System for Award Management (SAM) registration, and Grants.gov account to apply for grants. If individual applicants are eligible to apply for this grant funding opportunity, then you may begin with step 3, Create a Grants.gov account, listed below.

Creating a Grants.gov account can be completed online in minutes, but SAM registration may take several weeks. Therefore, an organization's registration should be done in sufficient time to ensure it does not impact the entity's ability to meet required application submission deadlines. Complete organization instructions can be found on Grants.gov here: https://www.grants.gov/web/grants/applicants/organization-registration.html.

i. **Register with SAM:** All organizations applying online through Grants.gov must register with the System for Award Management (SAM). Failure to register with SAM will prevent your organization from applying through Grants.gov. SAM registration must be renewed annually. Organizations will be issued a UEI number with the completed SAM registration.

   For more detailed instructions for registering with SAM, refer to: https://www.grants.gov/web/grants/applicants/organization-registration/step-2-register-with-sam.html.

ii. **Create a Grants.gov Account:** The next step is to register an account with Grants.gov. Follow the on-screen instructions or refer to the detailed instructions here: https://www.grants.gov/web/grants/applicants/registration.html.

iii. **Add a Profile to a Grants.gov Account:** A profile in Grants.gov corresponds to a single applicant organization the user represents (i.e., an applicant) or an individual applicant. If you work for or consult with multiple organizations and have a profile for each, you may log in to one Grants.gov account to access all of your grant applications. To add an organizational profile to your Grants.gov account, enter the UEI Number for the organization in the UEI field while adding a profile. For more detailed instructions about creating a profile on Grants.gov, refer to: https://www.grants.gov/web/grants/applicants/registration/add-profile.html.

iv. EBiz POC Authorized Profile Roles: After you register with Grants.gov and create an Organization Applicant Profile, the organization applicant's request for Grants.gov roles and access is sent to the EBiz POC. The EBiz POC will then log in to Grants.gov and authorize the appropriate roles, which may include the AOR role, thereby giving you permission to complete and submit applications on behalf of the organization. You will be able to submit your application online any time after you have been assigned the AOR role. For more detailed instructions about creating a

profile on Grants.gov, refer to: https://www.grants.gov/web/grants/applicants/registration/authorize-roles.html.

v. **Track Role Status:** To track your role request, refer to: https://www.grants.gov/web/grants/applicants/registration/track-role-status.html.

vi. **Electronic Signature:** When applications are submitted through Grants.gov, the name of the organization applicant with the AOR role that submitted the application is inserted into the signature line of the application, serving as the electronic signature. The EBiz POC **must** authorize people who are able to make legally binding commitments on behalf of the organization as a user with the AOR role; **this step is often missed, and it is crucial for valid and timely submissions.**

8. How to Submit an Application to DHS via Grants.gov

Grants.gov applicants can apply online using Workspace. Workspace is a shared, online environment where members of a grant team may simultaneously access and edit different webforms within an application. For each NOFO, you can create individual instances of a workspace.

Below is an overview of applying on Grants.gov. For access to complete instructions on how to apply for opportunities using Workspace, refer to: https://www.grants.gov/web/grants/applicants/workspace-overview.html.

a. **Create a Workspace:** Creating a workspace allows you to complete it online and route it through your organization for review before submitting.
b. **Complete a Workspace:** Add participants to the workspace to work on the application together, complete all the required forms online or by downloading PDF versions, and check for errors before submission. The Workspace progress bar will display the state of your application process as you apply. As you apply using Workspace, you may click the blue question mark icon near the upper-right corner of each page to access context-sensitive help.
c. **Adobe Reader:** If you decide not to apply by filling out webforms you can download individual PDF forms in Workspace. The individual PDF forms can be downloaded and saved to your local device storage, network drive(s), or external drives, then accessed through Adobe Reader.

   NOTE: Visit the Adobe Software Compatibility page on Grants.gov to download the appropriate version of the software at: https://www.grants.gov/web/grants/applicants/adobe-software-compatibility.html.
d. **Mandatory Fields in Forms:** In the forms, you will note fields marked with an asterisk and a different background color. These fields are mandatory fields that must be completed to successfully submit your application.
e. **Complete SF-424 Fields First:** The forms are designed to fill in common required fields across other forms, such as the applicant's name, address, and UEI number. To trigger this feature, an applicant must complete the SF-424 information first. Once it is completed, the information will transfer to the other forms.
f. **Submit a Workspace:** An application may be submitted through workspace by clicking the Sign and Submit button on the Manage Workspace page, under the Forms tab.

Grants.gov recommends submitting your application package at least 24-48 hours prior to the close date to provide you with time to correct any potential technical issues that may disrupt the application submission.

g. **Track a Workspace Submission:** After successfully submitting a workspace application, a Grants.gov Tracking Number (GRANTXXXXXXXX) is automatically assigned to the application. The number will be listed on the Confirmation page that is generated after submission. Using the tracking number, access the Track My Application page under the Applicants tab or the Details tab in the submitted workspace.

For additional training resources, including video tutorials, refer to: https://www.grants.gov/web/grants/applicants/applicant-training.html.

Applicant Support: Grants.gov provides applicants 24/7 support via the toll-free number 1-800-518-4726 and email at support@grants.gov. For questions related to the specific grant opportunity, contact the number listed in the application package of the grant to which you are applying.

If you are experiencing difficulties with your submission, it is best to call the Grants.gov Support Center and get a ticket number. The Support Center ticket number will assist DHS with tracking your issue and understanding background information on the issue.

9. Timely Receipt Requirements and Proof of Timely Submission

a. **Online Submission.** All applications must be received by 11:59 P.M. Eastern time on the due date. Proof of timely submission is automatically recorded by Grants.gov. An electronic date/time stamp is generated within the system when the application is successfully received by Grants.gov. The applicant with the AOR role who submitted the application will receive an acknowledgement of receipt and a tracking number (GRANTXXXXXXXX) from Grants.gov with the successful transmission of their application. This applicant with the AOR role will also receive the official date/time stamp and Grants.gov Tracking number in an email serving as proof of their timely submission.

When DHS successfully retrieves the application from Grants.gov, and acknowledges the download of submissions, Grants.gov will provide an electronic acknowledgment of receipt of the application to the email address of the applicant with the AOR role who submitted the application. Again, proof of timely submission shall be the official date and time that Grants.gov receives your application. Applications received by Grants.gov after the established due date for the program will be considered late and will not be considered for funding by DHS.

Applicants using slow internet, such as dial-up connections, should be aware that transmission can take some time before Grants.gov receives your application. Again, Grants.gov will provide either an error or a successfully received transmission in the form of an email sent to the applicant with the AOR role attempting to submit the application. The Grants.gov Support Center reports that some applicants end the transmission because they think that nothing is occurring during the transmission process. Please be patient and give the system time to process the application.

10. Content and Form of Application Submission

All applications must submit all required forms and required documents listed in this section. Applications missing any of the required forms or documents listed in this section may not be considered for review. The Project Narrative is limited to 25 double-spaced single-sided 8.5 x 11-inch pages with Times New Roman 12-point text font and 1-inch margins. You must number the Project Narrative beginning with page number 1. We will not read or consider any materials beyond the specified page limit in the application review process. The Budget and Budget Narrative do not count against the page limit requirements for the Project Narrative.

The following instructions provide all the information needed to complete the Budget, Budget Narrative and Project Narrative. Carefully read and consider each section below and include all required information in your application. The agency will evaluate the submitted content using the evaluation criteria identified in Section E.1. You must use the same section headers identified below for each section of the Budget Narrative and Project Narrative. The maximum possible score is 100 points.

a. REQUIRED FORMS

i. Form SF-424 – Application for Federal Assistance

Complete the SF-424 application form. This form may be completed on the Grants.gov website or it can be completed offline in its entirety.

NOTE: Applications submitted through Grants.gov must use the SF-424 provided by Grants.gov. The SF-424 application forms can only be viewed and downloaded once Adobe Reader has been installed. The SF-424 application form on Grants.gov is formatted so applicants are only required to complete fields which are indicated with an asterisk (*) and color coded. Once the application is complete, close the document (you will then be prompted to save changes or not).

ii. Form SF-424A – Budget

Complete the budget in its entirety. Provide budget amounts by object class (salaries, fringe, travel, indirect, etc.). Funds may be requested if the item and amount are necessary to perform the proposed work and are not precluded by the cost principles or program funding restrictions. Additional guidance on how to complete the Form SF-424A can be found at: http://www.grants.gov/web/grants/forms.html

iii. Budget Narrative (Maximum of 10 points)

The Budget Narrative must provide a description of costs associated with each line item on the SF-424A. The Budget Narrative should also include a section describing any leveraged resources provided (as applicable) to support cooperative agreement activities. Leveraged resources are all resources, both cash and in-kind, in excess of this award. Applicants are encouraged to leverage resources to increase stakeholder investment in the project and broaden the impact of the project itself. Each category should include the total cost for the period of performance. Use the following guidance for preparing the Budget Narrative.

The Budget Narrative should address how the funds allocated to each eligible activity will be spent and how costs were determined for the following cost purposes:

1) **Planning Costs** ***(2 points)*** The Budget Narrative must identify the planning activities on which proposed costs will be spent each year. Provide detail on proposed activities.
2) **Personnel and Contractual Costs** ***(2 points)*** The Budget Narrative must include any personnel costs of staff who support the development and implementation of the training program including, employee fringe benefit costs, travel costs, and supplies. Additional items, such as contractual costs for any goods and services, must also be included.
3) **Delivery Costs** ***(4 points)*** The Budget Narrative must provide detail on proposed numbers of students to benefit from the cybersecurity curriculum, number of education hours, anticipated location of training, outputs expected.
4) **Equipment Purchase Costs** ***(2 points)*** Each activity that proposes equipment purchase must provide a line-item cost breakout of equipment, including equipment description, unit cost, and quantity proposed for purchase. All equipment purchases will be reviewed by the Program Office.

iv. Program Narrative (Maximum of 90 points)

The Program Narrative must demonstrate the applicant's capability to implement the objectives of the cooperative agreement in accordance with the provisions of this announcement. It provides a comprehensive framework and description of all aspects of the proposed program. It must be succinct, self-explanatory, and well-organized so that reviewers can understand the proposed approach. The application must include a program narrative that provides a detailed overview description of the proposed efforts and thoroughly addresses the objectives. Provide or describe the following:

1) Organizational Information (6 points)

- Organization's name, mission, organizational structure, and the capacity to support the project by leading the development of training, apprenticeship, and employment placement activities within at least one local/regional area. ***(3 points)***
- A summary introduction/overview of the project's goals. ***(1 point)***
- Contact information, to include the name, title, address, email, and phone number of the primary contact and his/her back up. ***(2 points)***
- Applicants must provide information confirming its status as a nonprofit organization, other than institutions of higher education, described under section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from tax under section 501(a) of such code, or nonprofit organizations, other than institutions of higher education, that are not described under section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from tax under section 501(a) of such code. Any of the following is acceptable evidence of nonprofit status: (a) a reference to the applicant organization's listing in the

Internal Revenue Service's (IRS) most recent list of tax-exempt organizations described in section 501(c)(3) of the IRS Code; (b) a copy of a currently valid IRS tax exemption certificate; (c) a statement from a State taxing body, State Attorney General, or other appropriate State Official certifying that the applicant organization has a nonprofit status and that none of the net earnings accrue to any private shareholders or individuals; (d) a certified copy of the organization's certificate of incorporation or similar document that clearly establishes nonprofit status; (e) any of the above proof for a State or national parent organization and a statement signed by the parent organization that the applicant organization is a local nonprofit affiliate.

2) **Communities Served (4 points)** Applicants must provide a clear identification and description of the specific target communities that will be served, as identified in Section C.2.a. Target Community. The description of target communities must include demographic characteristics as identified in Section C.3.a. Target Audience and an explanation of how the target audience will meet and benefit from the requirements of this cooperative agreement.

3) **Jurisdictional and Geographic Area(s) (2 points)** Applicants must provide the county or other equivalent jurisdiction in which the program is located and any other counties or jurisdictions that will benefit.

4) **Past Performance (13 points)**
Full description of the applicant's proven past performance in leading the development of training, apprenticeship, and employment placement activities within at least one local/regional area during the performance period for the grant/cooperative agreement. This could include evidence of the applicant managing federally and/or non-federally funded assistance agreements leading engagement strategies, or other activities similar in size, scope, and relevance to the proposed project within the last five years, as of the closing date of this Announcement. ***(4 points*)**
   - Demonstration that applicants have experience in developing and implementing cybersecurity training and placement programs for the target communities identified in Section C.2 Applicant Eligibility Criteria and enrolling participants in those training programs, including securing employment placements for entry-level or higher-skilled cybersecurity jobs. ***(4 points)***
   - Applicants must submit, as part of their past performance, the total grant/cooperative agreement amount, and the percentage of funds spent during the period of performance for their most recently completed grant or cooperative agreement, where applicable. Applicants will receive points for their spending rate. ***(4 points)***

- Applicants that expended at least 98% of the award funds for their most recently completed grant/cooperative agreement will receive. ***(4 points)***
- Applicants that expended at least 80% but less than 98% of the award funds for their most recently completed grant will receive. ***(2 points)***
- Applicants that expended less than 80% of the award funds for their most recently completed grant will receive. ***(0 points)***

- Applicants must provide past performance data related to outputs and associated outcomes that were achieved in past related initiatives. ***(1 point)***
  NOTE: Past performance documentation shall include:
  - Grantor name and contact information
  - Project/program information
  - Grant objectives
  - Performance goals
  - Spending rate analysis
  - Overall objectives of the grant
  - Community served
  - Funding amount
  - Total number of participants who completed training and apprenticeship activities
  - Total number of participants who completed training and apprenticeship activities and secured full-time employment

5) Proposed Design (45 points)

Scoring is based on the measurable standards below which assess a proposed design and implementation plan. For the purpose of scoring, applicants must describe a clear, realistic plan (to include proposed outreach, training and placement services designed to assist underserved participants to successfully be placed into entry-level cybersecurity jobs and aligned with the Allowable Activities in Section A.9.d. in a narrative format and include the following requirements:

- ***Cybersecurity Pathways Retention Strategy (8 points)***
  - Thorough description of how the proposed training hub and apprenticeship/employment placement activities for the program will meet the needs of employers and support the achievement of the proposed training and apprenticeship outputs/outcomes. ***(1 point)***
  - Thorough description of recruiting strategies to meet the proposed number of participants and provide a thorough description of the assessment process to determine if individuals are an appropriate fit for the training and apprenticeship activities. ***(1 point)***
  - Thorough and convincing description of how the proposed training and apprenticeship activities are appropriate for the target communities to be served, as described in Section C.2. Applicant Eligibility Criteria, and how the strategies will address skills, training gaps, and other needs of participants identified. ***(1 point)***

- The extent to which the participant is relieved of any financial burden or is compensated. ***(1 point)***
- Clear description of how feedback and output measures can be collected in areas, potentially without internet access. ***(1 point)***
- Outline any anticipated challenges to developing and implanting a training hub and apprenticeship/employment program including proposed resolutions to ensure effective delivery and continuity of the effort. ***(1 point)***
- Clear description of any additional measures (if identified) that support success in entry-level cybersecurity training, apprenticeships, and job placement. ***(1 point)***
- Clear description of how the proposal can generate best practices and lessons learned for other underserved communities with similar needs. ***(1 point)***

- ***Professional Network (15 points)***
  - A clear description of the applicant's existing professional cybersecurity network, including the entity's name and length of the working relationship. For full points, applicants must clearly demonstrate the active involvement of the required workforce partnership entities by attaching partnership agreements, organizational charters, memorandum of understanding (MOU), letter of intent (LOI), or other types of signed agreements or acknowledgements. ***(5 points)***
  - An overview of the joint efforts related to training and placement that have been accomplished as a result of the applicant's existing professional cybersecurity network. ***(5 points)***
  - Thorough description of how any partner organizations/affiliations identified in Sections C.3 Other Eligibility Criteria/Restrictions (Required Partners and Optional Affiliates) will support the proposed training hub and apprenticeship/employment placement activities for the program and the process to ensure collaboration between all entities. ***(5 points)***

- ***Training Hub Design (22 points)***
  - A clear description of the training hub's design, which must be aligned with the work roles outlined in the NICE Framework, offered either in-person, virtually or a hybrid combination of both, and increase engagement by connecting participants and employers in one or more CISA regions. ***(2 points)***
  - Clear description of how the curricula and training strategies will be updated over time as employers' needs change. ***(2 points)***
  - Clear description of how the proposed training hub will successfully promote the cybersecurity training hub and entry-level employment opportunities to one or more underserved communities, including though an online web presence. ***(2 points)***

- A clear description of how the proposed training hub design will be used to deliver entry-level cybersecurity training (covering both national and regional cybersecurity challenges) to underserved communities. ***(2 points)***
- Thorough explanation of innovative delivery (virtual, in person or a hybrid of both) of education and training that reflects the use of current technology-enabled strategies and, where appropriate, leverages existing standards, assessments, and curricula that have proven effectiveness. ***(2 points)***
- Clear description of the high-quality training strategies (computer-based and/or work-based), including the number of courses, that will be used to serve the targeted communities. This includes strategies such as Customized Cohort Training, Registered Apprenticeships, Industry-Recognized Apprenticeships, and other types of training. ***(2 points)***
- Clear description of career pathway strategies including planned and sequenced coursework, training and/or apprenticeship experience that leads to competitive skills for securing entry-level cybersecurity jobs. ***(2 points)***
- Clear description of how participants' knowledge, skills, and abilities will be measured throughout the training and apprenticeship, given the parameters of a virtual or hybrid in-person design. ***(2 points)***
- A clear description of how program participants will be introduced to cybersecurity career options aligned to the NICE Framework to include sample job roles and responsibilities. ***(2 points)***
- Thorough explanation of how the anticipated outputs are reasonable and appropriate numerical targets for the task specifically detailing how the targets were derived. ***(2 points)***
- A description of how the proposal will provide sharable versions of NICE Framework-mapped curricula used for this program. ***(2 points)***

6) Management Strategy (15 points)

Describe the organization's ability to effectively comply with the requirements of the grant and manage all aspects of this award in the following areas:

- ***Project Oversight (10 Points)***
  - Qualifications and capabilities of the Project Manager(s) assigned to the activity/task. ***(1 point)***
  - Qualifications and capabilities of the identified key personnel (at a minimum a Lead Educator, Communications/Marketing Lead and Placement Coordinator/Manager) who will manage and/or implement the proposed program. ***(3 points)***
  - The extent to which the Program Manager and identified key personnel have direct experience with and oversight of the management of a scalable approach to entry-level cybersecurity training, apprenticeships, and job placement in a cybersecurity career. ***(4 point)***
  - The extent to which the applicant has experience overseeing and monitoring the progress of Federally funded projects. ***(2 point)***

- ***Data Collection and Reporting Systems (3 Points)*** Comprehensive description of the existing or planned systems and processes that the applicant will use to provide timely and accurate performance reporting including the process for tracking participant-level data (related to program enrollment and progression, student demographics, and their employment status), professional network/placement pipeline development and alignment of the training hub to the work roles outlined in the NICE Framework. (CISA encourages applicants to use existing systems).

- ***Financial Tracking and Reporting Systems (2 Points)*** Comprehensive description of the existing or planned accounting systems and processes that the applicant will use to monitor the financial status of the project relative to the implementation timeline and provide timely and accurate financial reports.

7) Work Plan (5 points)

In conjunction with your program narrative, use the Work Plan template found in Appendix B to outline the organizations strategy for achieving the objectives of the program. The proposed efforts should directly relate to the Allowable Activities in Section A.9.d. and be supported by individual tasks that are necessary to complete those Activities as well as anticipated completion date and output targets. The table should include, at a minimum:

- the proposed task to accomplish the Allowable Activity ***(1 point)***
- lead personnel responsible for completion of the task (project manager, project officer, communications director, etc.). If a sub-awardee will be utilized to assist in accomplishing an activity/task, provide the name of the company/individual (if known) ***(1 point)***
- total budget ***(1 point)***
- estimated completion date ***(1 point)***
- anticipated output(s) ***(1 point)***

11. Other Submission Requirements

a. Deadlines. DHS will not accept late applications. Without exception, applications must be received by Grants.gov on or before the deadline in this announcement or they will not be considered.

b. Application Relevance. Applications that do not address the purpose of this announcement will not be considered.

c. Compliance and Completeness. Applications must substantially comply with the application submission instructions and requirements in this announcement, or they will not be considered.

d. Funding Limits. Applications requesting federal funding that exceeds the Maximum Award Amount will not be considered

12. Intergovernmental Review

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.

(See *https://www.archives.gov/federal-register/codification/executive-order/12372.html; https://www.whitehouse.gov/wp-content/uploads/2019/02/SPOC-February-2019.pdf*).

13. Funding Restrictions

a. DHS cooperative agreement funds may only be used for the purpose set forth in the terms of this Federal award, which include the terms of this NOFO and must be consistent with the statutory authority for the award. Cooperative agreement funds and non-monetary support under this NOFO may not be used for matching contributions for other federal grants or cooperative agreements, lobbying, or intervention in federal regulatory or adjudicatory proceedings. Federal employees are prohibited from serving in any capacity (paid or unpaid) on any proposal submitted under this program. Federal employees may not receive funds under this award. In addition, federal funds may not be used to sue the Federal Government or any other government entity. DHS substantial programmatic involvement and performance/progress reviews may result in funding restrictions in conjunction with initial and/or annual continuation awards.

b. Applicants must adhere to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200.

14. Allowable Costs

a. Pre-Award Costs

Pre-award costs are not permitted and, if accrued, will not be reimbursed.

b. Management and Administration (M&A) Costs *(if applicable)*

These costs are allowable by the recipient and sub-recipient. M&A are not operational costs but are necessary costs incurred in direct support of the cooperative agreement or because of it, such as travel, meeting-related expenses, and salaries of full/part-time staff in direct support of the program. Apprentices may be paid a stipend. As such these can be itemized in financial reports.

M&A costs are allowed for both the recipient and subrecipients. A recipient may use up to 5% of the federal award for M&A purposes. In addition, a subrecipient may use up to 5% of the amount they receive from the recipient under a subaward for M&A purposes. M&A costs and activities are not operational costs; they are costs and activities incurred in direct support of the cooperative agreement or as a result of the cooperative agreement and should be allocated across the entire lifecycle of the cooperative agreement. They are directly related to managing and administering the federal award, such as financial management, reporting, and program and financial monitoring. It should be noted that salaries of a recipient's personnel are not typically categorized as M&A costs unless the recipient chooses to assign personnel to specific M&A activities

c. Indirect Facilities & Administrative (F&A) Costs

Indirect Costs are allowable for the recipient and any proposed sub-recipient *(if*

applicable). **The applicant must attach a copy of the latest indirect cost rate agreement negotiated with a cognizant federal agency.** If the applicant is in the process of initially developing or renegotiating a rate, upon notification that an award will be made, it should immediately develop a tentative indirect cost rate proposal based on its most recently completed fiscal year, in accordance with the cognizant agency's guidelines for establishing indirect cost rates and submit it to the cognizant agency. Applicants awaiting approval of their indirect cost proposals may also request indirect costs. When an indirect cost rate is requested, those costs included in the indirect cost pool should not also be charged as direct costs to the award. If the applicant is requesting a rate which is less than what is allowed under the program, the authorized representative of the applicant organization must submit a signed acknowledgement that the applicant is accepting a lower rate than allowed.

Any non-Federal entity that has never received a negotiated indirect cost rate (except for those non-federal entities described in Appendix VII to Part 200 States and Local Government and Indian Tribe Indirect Cost Proposals, paragraph D.1.b) may elect to charge a de minimis rate of 10% of modified total direct costs (MTDC) which may be used indefinitely. As described in §200.403 Factors Affecting Allowability of Costs, costs must be consistently charged as either indirect or direct costs but may not be double charged or inconsistently charged as both. If chosen, this methodology once elected must be used consistently for all federal awards until such time as a non-federal entity chooses to negotiate for a rate, which the non-federal entity may apply to do at any time. For more information, see 2 CFR Part 200.414.

E. Application Review Information

1. Application Evaluation Criteria

a. Programmatic Criteria

The application requires the applicant to describe its existing capabilities and its plan to facilitate the successful implementation of the program. A well-described and thought-out plan is vital to the success of this program. For this reason, the application will be evaluated primarily based upon the applicant's approach to the program's implementation, demonstrating its understanding of this announcement's objectives, the plan for implementing and successfully demonstrating these objectives, and the reasonableness of this plan. In particular, the applicant must address how it meets the eligibility criteria listed above and provide evidence demonstrating this eligibility. If the application fails to address each of the evaluation criteria listed in the above scored sections, the applicant will be deemed ineligible and will not be selected.

The Cybersecurity and Infrastructure Security Agency (CISA) is the entity responsible for organizing the Objective Review Panel and the final selection process. When all applications are received, reviews will be conducted to confirm the Eligibility Information (see Section C) and Application and Submission Information (see Section D) listed in this NOFO are met. Applications meeting those requirements will then be reviewed by subject matter experts (SMEs) participating in the merit review panel. The merit review will focus on the overall quality of the proposed program and the

completion and thoroughness of the program narratives and budget narratives. The review panel will determine whether the proposal addresses the Cybersecurity Workforce Development and Training Program for Underserved Communities Program Objectives listed in Section A of this NOFO and will use the scoring criteria outlined in Section D.10 above (and summarized below) to evaluate applications.

i. Budget Narrative (10 Total Points)
ii. Program Narrative (90 Total Points)
    1. Organizational Information (6 points)
    2. Communities Served (4 points)
    3. Jurisdictional and Geographic Area(s) (2 points)
    4. Past Performance (13 points)
    5. Proposed Design (45 points)
    6. Management Strategy (15 points)
    7. Work Plan (5 points)

b. Financial Integrity Criteria

Prior to making a federal award, the DHS Grants and Financial Assistance Division is required by The Payment Integrity Act of 2019, 41 U.S.C. § 2313 – Database for federal agency contract and grant officers and suspension and debarment officials, and 2 C.F.R. §200.206 to review information available through any OMB-designated repositories of government wide eligibility qualification or financial integrity information. Therefore, application evaluation criteria may include the following risk-based considerations of the applicant:

i. Financial stability.
ii. Quality of management systems and ability to meet management standards.
iii. History of performance in managing federal award.
iv. Reports and findings from audits.
v. Ability to effectively implement statutory, regulatory, or other requirements.

c. Supplemental Financial Integrity Criteria and Review

Prior to making a federal award where the anticipated total federal share will be greater than the simplified acquisition threshold, currently $250,000 (see Section 805 of the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, OMB Memorandum M-18-18 at https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-18.pdf):

i. DHS Grants and Financial Assistance Division is required to review and consider any information about the applicant that is in the designated integrity and performance system accessible through SAM, which is currently the Federal Awardee Performance and Integrity Information System (FAPIIS) and is accessible through the sam.gov website.
ii. An applicant, at its option, may review information in FAPIIS and comment on any information about itself that a federal awarding agency previously entered.
iii. DHS Grants and Financial Assistance Division will consider any comments by the applicant, in addition to the other information in FAPIIS, in making a judgment about the applicant's integrity, business ethics, and

record of performance under federal awards when completing the review of risk posed by applicants as described in 2 C.F.R. §200.206.

2. Review and Selection Process

The Cybersecurity Workforce Development and Training Program for Underserved Communities review process will involve two review phases. First, all applications will be reviewed to confirm eligibility and completeness. Then, a panel of federal employees and SMEs knowledgeable in cybersecurity entry-level and awareness training, will review the applications and determine a merit score. The merit score will be based on the degree to which an application addresses the Application Evaluation Criteria listed above (see Section F.1.). DHS will review the applications and recommend for funding based on the reviews described above. DHS' designated Selection Authority will make a final funding decision to implement the demonstration project(s) based upon the results of all evaluations, availability of funds, and the overall goals of Cybersecurity Workforce Development and Training Program for Underserved Communities Program.

In addition, DHS will also review the budget narrative to ensure proposed cost estimates are in line with eligible costs and available program funding. Prior to making a federal award with a total amount of federal share greater than the simplified acquisition threshold, DHS is required to review and consider any information about the applicant that is in the designated integrity and performance system accessible through SAM (currently FAPIIS).
An applicant, at its option, may review information in the designated integrity and performance systems accessible through SAM and comment on any information about itself that a federal awarding agency previously entered and is currently in the designated integrity and performance system accessible through SAM.

DHS will consider any comments by the applicant, in addition to the other information in the designated integrity and performance system, in making a judgment about the applicant's integrity, business ethics, and record of performance under federal awards when completing the review of risk posed by applicants as described in 2 C.F.R. § 200.205 federal awarding agency review of risk posed by applicants."

F. Federal Award Administration Information

1. Notice of 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 as well as any special terms and conditions in the Notice of Award to receive an award under this program.***

DHS issues formal award notification documents following fulfillment of DHS Congressional notifications. All DHS grants and cooperative agreements are subject to the standard DHS Award Terms and Conditions, which are attached to this package.
A grant award will be executed by a DHS Grants Officer authorized to obligate DHS funding. Unsuccessful applicants will be contacted as well and will be encouraged to apply

for future grant award programs. Announcements for future programs will be listed at http://www.grants.gov.

2. Administrative and National Policy Requirements

All successful applicants for DHS grant and cooperative agreements are required to comply with DHS Standard Terms and Conditions, which are available online at: DHS Standard Terms and Conditions.

The applicable DHS Standard Terms and Conditions will be those in effect at the time the award was made unless the application is for a continuation award. In that event, the terms and conditions in effect at the time the original award was made will generally apply. What terms and conditions will apply for the award will be clearly stated in the award package at the time of award.

3. Reporting

a. Federal Financial Reporting Requirements

The Federal Financial Report (FFR) form is available online at: SF-425 *OMB #4040-0014*

The Recipient is required to submit the following financial reports:

Quarterly Federal Financial Reports (SF-425) must be submitted to the DHS Grants Officer within 30 days after the end of each quarter. Reports are due January 30, April 30, July 30, and October 30. Reports shall be submitted via the Grants Solution System.

Quarterly Federal Financial Reports (Cash Transaction) the Recipient shall submit the FFR (SF-425) Federal Cash Transaction Reports to the Department of Health and Human Services, Payment Management System. Quarterly Cash Transaction reports shall be submitted no later than January 30, April 30, July 30, and October 30 of each year.

b. Programmatic Performance Reporting Requirements

The recipient is required to submit the following performance reports:

Semi-Annual Performance Reports Award recipients will receive a Performance Progress Report (PPR) Template that must be submitted to the CISA Program Officer no later than 30 days after the end of the semi-annual reporting period. Reports are due April 30 (for September – March) and October 30 (for April-September)**.** Reports must be submitted via the GrantSolutions.gov feature using the **guidance** found here: https://www.grantsolutions.gov/support/granteeUsers.html.

The PPR Template will evaluate progress and program success by requiring awardees to report on:

- Activity/Task updates inclusive of any deviations from the approved Work Plan, milestone achievements (or lack thereof), Performance Measure tracking and

additional performance metrics to support them including relevant participant demographic data, where applicable; unanticipated challenges and strategy for overcoming them and program successes.

- An updated Work Plan, as applicable
- Programmatic expenditures and/or deviations from the approved project budget categorized by both object class and project.
- If applicable, include a certification that no patentable inventions were created during the budget periods.
- If the performance report contains any information that is deemed proprietary, the Recipient will denote the beginning and ending of such information w the following heading: *PROPRIETARY INFORMATION*

c. 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 grant, recipients must submit the following:

I. The final request for payment, if applicable.

II. The final FFR (SF-425).

III. The final progress report detailing all accomplishments.

IV. A qualitative narrative summary of accomplishments or innovations throughout the period of performance, including:

1. Training strategies and new approaches to employer engagement.

2. A description of how the implementation of the program yielded proof or evidence that will enable the broader workforce system to replicate the outcomes of the performance measures.

3. A description of outcomes, data collection methods, and feedback mechanisms used to assess the efficacy of the program.

4. A description of how any training, apprenticeship, and/or employment barriers were addressed.

5. Other documents required by this NOFO, terms and conditions of the award, or other DHS Grants and Financial Assistance Division guidance.

After these reports have been reviewed and approved by DHS Grants and Financial Assistance Division, a closeout notice will be completed to close out the grant. The notice will indicate the period of performance as closed, list any remaining funds that will be de-obligated, and address the requirement of maintaining the grant records for three years from the date of the final FFR, 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.

In addition, any recipient that issues subawards to any subrecipient is responsible for closing out those subawards as described in 2 C.F.R. § 200.344. Recipients acting as pass-through entities must ensure that they complete the closeout of their subawards in time to submit all necessary documentation and information to DHS Grants and Financial Assistance Division during the closeout of their prime grant award.

The recipient is responsible for returning any funds that have been drawn down but remain as unliquidated on recipient financial records.

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

This reporting requirement pertains to disclosing information related to government-wide suspension and debarment requirements. Before a recipient enters a cooperative agreement award with DHS Grants and Financial Assistance Division the recipient must notify DHS Grants and Financial Assistance Division if it knows if it or any of the recipient's principals under the award fall under one or more of the four criteria listed at 2 C.F.R. § 180.335:

- **i.** Are presently excluded or disqualified.
- **ii.** Have been convicted within the preceding three years of any of the offenses listed in 2 C.F.R. § 180.800(a) or had a civil judgment rendered against it or any of the recipient's principals for one of those offenses within that time period.
- **iii.** Are presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with commission of any of the offenses listed in 2 C.F.R. § 180.800(a).
- **iv.** Have had one or more public transactions (federal, state, or local) terminated within the preceding three years for cause or default.

At any time after accepting the award, if the recipient learns that it or any of its principals falls under one or more of the criteria listed at 2 C.F.R. § 180.335, the recipient must provide immediate written notice to DHS Grants and Financial Assistance Division in accordance with 2 C.F.R. § 180.350.

e. Reporting of Matters Related to Recipient Integrity and Performance

Per 2 C.F.R. Part 200, Appendix I § F.3, the additional post-award reporting requirements in 2 C.F.R. Part 200, Appendix XII may apply to applicants who, if upon becoming recipients, have a total value of currently active grants, cooperative agreements, and procurement contracts from all federal awarding agencies that exceeds $10,000,000 for any period during the period of performance of an award under this funding opportunity. Recipients that meet these criteria must maintain current information reported in FAPIIS about civil, criminal, or administrative proceedings described in paragraph 2 of Appendix XII at the reporting frequency described in paragraph 4 of Appendix XII.

f. Monitoring and Oversight

Per 2 C.F.R. § 200.329, DHS Grants and Financial Assistance Division, through its authorized representatives, has the right, at all reasonable times, to conduct desk reviews, make site visits to review project accomplishments and management control systems to review project accomplishments and to provide any required technical assistance. During site visits, DHS Grants and Financial Assistance Division will review grant recipients' files related to the grant award. As part of any monitoring and program evaluation activities, grant recipients must permit DHS Grants and Financial Assistance Division, upon reasonable notice, to review grant-related records and to interview the organization's staff and contractors regarding the program. Recipients must respond in a

timely and accurate manner to DHS Grants and Financial Assistance Division requests for information relating to the grant program**.**

g. Program Evaluation

Recipients and subrecipients are encouraged to incorporate program evaluation activities from the outset of their program design and implementation to meaningfully document and measure their progress towards the outcomes proposed. Title I of the Foundations for Evidence-Based Policymaking Act of 2018 (Evidence Act), Pub. L. No. 115-435 (2019) defines evaluation as "*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). Credible program evaluation activities are implemented with relevance and utility, rigor, independence and objectivity, transparency, and ethics (OMB Circular A-11, Part 6 Section 290).

Evaluation costs are allowable costs (either as direct or indirect), unless prohibited by statute or regulation, and such costs may include the personnel and equipment needed for data infrastructure and expertise in data analysis, performance, and evaluation. (2 C.F.R. §200).

In addition, recipients are required to participate in a DHS-led evaluation if selected, which may be carried out by a third-party on behalf of the Program Office or DHS. By accepting federal funds, recipients agree to participate in the evaluation, which may include analysis of individuals who benefit from the grant, and provide access to program operating personnel and participants, as specified by the evaluator(s) during the award.

G. DHS Awarding Agency Contact Information

1. Contact and Resource Information

****Questions about this NOFO should be directed to** education@cisa.dhs.gov ******

The **Grants Officer** is the DHS official that has the full authority to negotiate, administer and execute all terms and conditions of the federal award in concurrence with the Program Officer.

Sean Lilly
Office of Procurement Operations (MGMT OPO)
Grants and Financial Assistance Division
Phone: (202) 601-9303
Email: Sean.Lilly@hq.dhs.gov

The **Program Officer** is the CISA staff member responsible for monitoring the completion of work and technical performance of the federal award.

Ashley Pearce
Cybersecurity Infrastructure Security Agency
Cyber Defense Education & Training
Email: education@cisa.dhs.gov

H. Other Information

1. Period of Performance Extensions

Extensions to the Period of Performance can only be authorized in writing by the DHS Grants Officer.

The extension request shall be submitted to the DHS Grants Officer sixty (60) days prior to the expiration date of the performance period. Requests for time extensions to the Period of Performance will be considered, but will not be granted automatically, and must be supported by adequate justification to be processed. The justification is a written explanation of the reason or reasons for the delay; an outline of remaining resources/funds available to support the extended period of performance; and a description of performance measures necessary to complete the project. Without performance and financial status reports current and justification submitted, extension requests shall not be processed.

DHS has no obligation to provide additional resources/funding as a result of an extension.

Grants and Financial Assistance Division (GFAD) Disclosure

Risk Assessment Evaluation

DHS staff will evaluate the risks to the program posed by each applicant, including conducting due diligence to ensure an applicant's ability to manage federal funds. This evaluation is in addition to the evaluation of the applicant's eligibility and the quality of its application on the basis of the Selection Criteria, and results from this evaluation may assist funding decisions. If an award is made, DHS may apply special conditions that correspond to the degree of risk of the award.

In evaluating risks, DHS may consider the following:

- Financial stability;
- Quality of management systems and ability to meet the management standards prescribed in applicable OMB Guidance;
- Applicant's record in managing previous DHS awards, cooperative agreements, or procurement awards, including:

1. Timeliness of compliance with applicable reporting requirements
2. Accuracy of data reported
3. Conformance to the terms and conditions of previous federal awards
4. If applicable, the extent to which any previously awarded amounts will be expended prior to future awards
5. Information available through OMB-designated repositories of government-wide eligibility qualification or financial integrity information, such as: Federal Awardee Performance and Integrity Information System (FAPIIS), Duns and SAM

6. Reports and findings from single audits performed under Subpart F – Audit Requirements, 2 C.F.R. Part 200 and findings and reports of any other available audits
7. Applicant organization's annual report
8. Publicly available information, including information from the applicant organization's website
9. Applicant's ability to effectively implement statutory, regulatory, or other requirements imposed on award recipients.

In addition, organizations who have not received prior DHS Grants and Financial Assistance Division (GFAD) awards may be required to complete a risk assessment questionnaire as part of the pre-award financial and administrative review.

I. Appendices

APPENDIX A: WORK PLAN TEMPLATE

APPENDIX B: PERFORMANCE MEASURES

APPENDIX A: WORK PLAN TEMPLATE

Cybersecurity Workforce Development and Training Program for Underserved Communities
DHS NOFO Number: DHS-21-CISA-127-XXXXXXX
[Insert Applicant Organization Name]

FY23-25 WORK PLAN		Responsibility	Total Budget	Target Completion Date (or ongoing)	Anticipated Output
Example					
Activity A	***Draft a Cybersecurity Pathways Retention Strategy (CPRS) for underserved communities to be approved by CISA.***				
Task 1	*Convene meeting of key personnel and stakeholders to discuss planned execution and long-term commitment*	*Project Officer*	*$X,XXX*	*December 2023*	*Draft CPRS*
Activity X					
Task 1					
Task 2					
Activity X					
Task 1					
Activity X					
Task 1					
Task 2					
Task 3					
Task 4					

APPENDIX B: PERFORMANCE MEASURES

The following Performance Measures will be used to measure the success of the project during the award period. Applicants must include numerical output projections to evaluate the performance measures 1 and 2 and a percentage for performance measures 3 and 4. Applicants must provide raw numbers and percentages for each of the target measures. Percent increases, or other types of data projections, are not acceptable. Demographics for the performance measures pertaining to program enrollees/participants is also required and should include, where possible, age (range), gender, gender identity, race, ethnicity, education level, location (rural/sub-/urban) and/or sexual orientation.

Applicants shall provide performance measure targets for each specific Fiscal Year (not cumulative annual targets) within the period of performance as well as a cumulative target for the entire 3-year award period as shown in the example table below. Targets shall be developed (and reported) relative to achievable outputs resulting from funds awarded under this NOFO only. Performance and the associated outputs supported by other sources of funding (grants, cooperative agreements, charitable funding, donations, etc.) should not be considered.

Awardees will be required to provide updated annual and cumulative output targets throughout the project's period of performance, as applicable. CISA will use the targets to better track performance and provide technical assistance to recipients in an effort to support them in achieving their three-year output goals.

Additional metrics and relative demographic data that further supports these performance measures will be a required element of the Semi-Annual Performance Progress Report. It will be expected that, when reporting demographics, that they are associated with specific training courses and sections, as applicable. Award recipients will receive a Performance Progress Report Template to be submitted according to the frequency and schedule outlined in Section G.3.b.

PERFORMANCE MEASURES		END OF FISCAL YEAR TARGETS			CUMULATIVE
		FY23	FY24	FY25	3-YEAR TOTAL
1	Number of reciprocal arrangements (agreements, MOU, LOI, etc.) with employers who place program participants in apprenticeships and/or hire program graduates as full-time employees				
2	Number of underserved individuals enrolled in the training and placement program				
3	Percent of enrolled program participants who successfully obtain an apprenticeship				
4	Percent of enrolled program participants who graduate from the NTTP training program and successfully obtain full-time employment as a cybersecurity professional				