The Department of Homeland Security (DHS)
Notice of Funding Opportunity (NOFO)
CISA Cyber Security Awareness Campaign

All entities wishing to do business with the federal government must have a unique entity identifier (UEI). Entities that have done business with the government can obtain their UEI by following the steps here. Entities that have not done business with the federal government may request a UEI via the System for Award Management (SAM) web page at: https://sam.gov/content/entity-registration. Receiving a UEI take 1-2 business days.

Grants.gov registration information can be found at: https://www.grants.gov/web/grants/register.html. Detailed information regarding UEI and SAM is also provided in Section D of this NOFO.

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 Listings Number** 97.128

3. **Assistance Listings Title** Cyber Security Awareness.

4. **Funding Opportunity Title**
   CISA Cyber Security Awareness Month Campaign

5. **Funding Opportunity Number**
   DHS-22-CISA-128-CSA001

6. **Authorizing Authority for Program**
   Section 102(b)(2) of the Homeland Security Act of 2002, as amended
   (6 U.S.C. § 112(b)(2)).

7. **Appropriation Authority for Program**
   Department of Homeland Security Appropriation Act, 2022 (Public Law 117-103), Title III, Protection, Preparedness, Response, and Recovery, Cybersecurity and Infrastructure Security Agency, Operations and Support.

8. **Announcement Type**
   New

9. **Program Overview, Objectives, and Priorities**
   The Cybersecurity and Infrastructure Security Agency (CISA) serves as the Nation's risk advisor to build the national capacity to defend against cyber-attacks, identify and address the most significant risks to national critical functions, and coordinate security and resilience efforts across the public and private sectors that encompass our Nation's critical infrastructure.

   In accordance with the 2020-2024 DHS Strategic Plan (found at https://www.dhs.gov/publication/department-homeland-securitys-strategic-plan-fiscal-years-2020-2024), CISA supports the following DHS guiding principles:

   - Championing "Relentless Resilience" for All Threats and Hazards: DHS will remain resolute against today's threats and hazards by keeping pace with our adversaries and preparing for those of tomorrow by identifying and confronting systemic risk, ensuring the Nation's citizens remain resilient, building redundancy and resilience into community lifelines, and raising the baseline of our security across the board—and across the world.

   - Promote Citizen Engagement and Strengthen and Expand Trusted Partnerships: Homeland security is a whole-of-society endeavor, from every federal department and agency to every American across this Nation. We will work together and empower partners to leverage national capacity and capabilities, improve training exercises, and develop contingency plans that make America safe, secure, and resilient against all threats and all hazards.

   This grant specifically supports the following CISA Cyber Security Awareness Month Strategic Plan Goals:

   - Strengthen the security and resilience of critical infrastructure
   - Assess and counter evolving cybersecurity risks.
   - Build a National culture of preparedness
   - Support outcome-driven community recovery

Accordingly, coordination and collaboration with public and private sector entities is necessary to facilitate a comprehensive cybersecurity awareness campaign program. This Cybersecurity Awareness Month campaign program intends to execute a research-driven strategy focused on implementing specific programs, activities, materials and outreach efforts, building on its cybersecurity awareness campaign to include activities and initiatives associated with Cybersecurity Awareness Month in October 2022.

A comprehensive approach to CISA's Cybersecurity Awareness Month:

- Educate the public about the dangers of cyber threats and key actions that can be taken to mitigate risks;
- Identify effective approaches to increase cybersecurity awareness among the general public and target audiences;
- Build relationships and coalitions across cybersecurity stakeholders to support Cybersecurity Awareness Month;
- Execute means of measuring impact of Cybersecurity Awareness Month campaign strategies on increasing public cybersecurity awareness, and
- Serve to further the Administration's National Security Strategic priority to build a culture of preparedness, informing and empowering communities and individuals to obtain the skills and take the preparatory actions necessary to become more resilient against threats and hazards Americans face.

Cyber threats can be just as detrimental to communities, infrastructure, businesses, and individuals as a natural disaster. With this in mind, we should seek to improve the public's understanding of cyber threats as well as opportunities Americans leverage to strengthen their own cybersecurity posture.

The recipient will research, plan, execute and measure project or individual initiative-based activities as part of a holistic strategy to drive cybersecurity actions in the targeted audiences. Viable applicants must ensure they address capabilities and approach to driving behavior change among wide-ranging audiences.

As part of this work, the recipient will be required to organize, execute, and reach audiences with in-person events across the country, web-based outreach and use multiple media channels (from traditional media to social media).

The recipient must address how it will coordinate and collaborate with stakeholder groups in creative ways (e.g., current and potential Campaign partners), which span the public and private sectors. This includes how the recipient will amplify, promote, and bolster CISA's existing cybersecurity awareness work and CISA's Cybersecurity Awareness Month themes and messaging.

Strategy Development

- Assess current and future cybersecurity awareness needs for the general public as well as for targeted segments based on susceptibility to cyber threats and receptivity to adopting cybersecurity practices.
- Perform market research to determine target audiences' interests, needs and barriers to adopting cybersecurity best practices to inform design and execution of Cybersecurity Awareness Month to most effectively address cybersecurity risk.
- In coordination with CISA, develop an annual Cybersecurity Awareness Month campaign

- Measure, analyze and report on the effectiveness of awareness efforts and associated outcomes, to include:
  - Developing a methodology for measuring Cybersecurity Awareness Month outreach and outcomes.
  - Establishing baselines for awareness and actions associated with Cybersecurity Awareness Month
    - Conduct research to measure behavior changes due to Cybersecurity Awareness Month exposure/saturation in order to determine program effectiveness. Such research may include: Identification of changes influenced by campaign promotion and specific events or tactics executed
    - Analysis of broad shifts in public attitudes or policies, measured through independent studies, government surveys, or polls
    - Capturing the number of hits on websites and relevant social media platforms

Cybersecurity Awareness Month Materials Production

- In coordination with CISA, create aligned, visually engaging, action oriented and outcome driven cybersecurity awareness collateral that can be leveraged by diverse stakeholder groups and serve as a repository for cybersecurity awareness-related activities and collateral.
- Develop and execute creative website content and additional communication mediums for dissemination and promotion of cybersecurity messaging.

Stakeholder Engagement and Outreach

- Establish formal and informal partnerships with key cybersecurity stakeholder groups to reach target audiences and communities.
- Assist CISA in the development of a coordinated messaging effort with public and private sector partners.

Cross-promotion of Cybersecurity Resources

- Utilize and incorporate DHS/CISA cybersecurity programs/resources where applicable and relevant.
- Align awareness/outreach efforts to the CISA strategic plan for long-term success, and provide input to new and innovative ideas, content, and strategies for CISA's Cybersecurity Awareness Month.

Execute Cybersecurity Awareness Month Activities

- Design a strategy to engage partners and raise the visibility of Cybersecurity Awareness Month (October), to include tailored activities for specific audiences
- Facilitate partnerships to execute a comprehensive Cybersecurity Awareness Month campaign across a wide range of audiences and communications channels.
- Secure and conduct media engagement to promote cybersecurity awareness, and available resources to increase cybersecurity actions amongst the general public and target segments.
- Create, produce and disseminate Cybersecurity Awareness Month campaign materials to include partner toolkits, web content, public service announcements, social media content, graphics and print materials supporting identified themes.

- Plan and produce targeted events to promote the month in geographically diverse locations with a variety of themes and audience targets, including a "Cybersecurity Awareness Month kick-off" event.

Program Management

- Provide CISA with timely reports that accurately reflect the recipient's progress toward agreed-upon awareness program goals as determined by CISA and the recipient throughout the period of performance.
- Determine contingency plans for unexpected program changes.

10. Performance Measures

The recipient will show the impact CISA Cyber Security Awareness Campaign Grantee's activities have on the advancement of CISA goals, through cumulative year-end datasheet reporting of the following performance metrics:

- Strengthen the security and resilience of critical infrastructure
- Assess and counter evolving cybersecurity risks.
- Build a National culture of preparedness
- Support outcome-driven community recovery

10.1: Strengthen the security and resilience of critical infrastructure

o Number and list of Cybersecurity Awareness Campaign key messages offered related to cybersecurity occurrences to critical infrastructure information, technology systems and/or infrastructure control systems security

o Types of Cyber Security Awareness Campaign outreach engagements/instances targeted toward the critical infrastructure security stakeholder audience

o Actual or estimated number and demographic of critical infrastructure security community stakeholder groups reached through each type of outreach engagement/instance sorted by Critical Infrastructure Sector, CISA Region, State, Local, Tribal, Territorial, Private Sector, and International affiliation

10.2: Assess and counter evolving cybersecurity risks

o Number Cybersecurity Awareness Campaign key messages offered related to reducing cybersecurity risks

o Actual or estimated number and demographic of community stakeholder groups reached through each type of outreach engagement/instance sorted by CISA Region, Federal State, Local, Tribal, Territorial, Private Sector, and International Affiliation

10.3: Build a National culture of preparedness

o Number of Cybersecurity Awareness Campaign key communications related to general public

- Types of Cybersecurity Awareness Campaign outreach engagements/instances targeted toward the general public computer user audience
- Estimated number of general public reached through outreach
- Number and types of Cybersecurity Awareness Campaign measurement tools used to measure changes in behavior toward cybersecurity
- Percentage increase in the total number of Americans and International users receiving overall cybersecurity awareness campaign messaging from prior campaign years

10.4: Support outcome-driven community recovery

- Number of Cybersecurity Awareness Campaign key messages offered connected to specific community recovery activities following a cybersecurity incident
- Estimated number and demographic of community recovery stakeholders reached through each type of outreach engagement/instance, sorted by CISA Region, Federal, State, Local, Tribal, Territorial, Private Sector, and International affiliation
- Number of new DHS partnerships formed through Cybersecurity Awareness Campaign activities

B. Federal Award Information

1. **Available Funding for the NOFO:** $549,996.00

2. **Projected number of Awards *(Optional)*:** One (1)

3. **Period of Performance:** 12 Months

   Indicate if an extension to the period of performance is permitted.
   If extensions to the period of performance are allowable, refer the applicant to "Section H. Additional Information, Period of Performance Extensions," which should specify what steps recipients must follow and what information must be included in the justification for such a request to be considered.

4. **Projected Period of Performance Start Date(s):** 09/30/2022

5. **Projected Period of Performance End Date(s):** 09/29/2023

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

Due to substantial involvement, the best way to support the broad public purpose of enhanced cybersecurity awareness is through a cooperative agreement.

DHS Program Office Substantial Involvement

1. CISA will direct and facilitate the applicant's collaboration with CISA and DHS's key

cybersecurity awareness partners, including such collaboration associated with the development of consistent cybersecurity awareness messaging and related concepts. All communication with any office within DHS must be coordinated through the designated Program Officer.

2. CISA will facilitate the participation of DHS officials and subject matter experts in workshops, conferences, or other project-related events, including but not limited to National Cybersecurity Awareness Month events, as requested by the applicant. CISA will coordinate with the applicant as necessary on such participation.

3. CISA must review and approve project materials prior to dissemination for purposes of ensuring suitability and appropriateness of message, including:

a. Publications, brochures, presentation materials, products, documents, websites (or portions thereof), social media presence and activities, or other cybersecurity awareness collateral produced under this award announcement that is to be shared with the public. Forty-five (45) days prior to the publishing or releasing such material, the recipient must submit a complete draft to the DHS Program Officer for review, comment and approval.

b. Agendas for meetings, seminars, workshops and conferences. Sixty (60) days prior to the event, the recipient must submit draft agendas and handouts to the DHS Program Office for review and approval.

c. If the recipient receives an invitation to present related information at a conference that is not listed in the approved project or budget narrative justification, and the activity will further the objectives of the campaign, the recipient shall seek the designated Program Officer's review and approval of its participation. The recipient shall notify the Program Officer and Grants Officer in writing within three (3) business days of the receipt of any such invitation. The notification, which may be transmitted by email, will consist of, at minimum:

i. The invitation, and
ii. A written justification explaining how participation in the conference furthers the mission of the project funded by this Award.

C. <u>Eligibility Information</u>

1. Eligible Applicants

Nonprofits with 501(c)(3) IRS status, other than institutions of higher education
Financial assistance will be awarded through a competitive process. Eligible applicants will include public or private non-profit organizations, dedicated to promoting cybersecurity-related awareness and safe behavior online through creative website

content and additional communication mediums nationwide. CISA will not review applications that fail to meet the eligibility criteria.

2. Applicant Eligibility Criteria

1. **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.

2. **Application relevance.** Applications that do not address the purpose of this announcement will not be considered.

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

4. **Funding limits.** Applications exceeding the funding limits will not be considered.

5. **Proof of non-profit status**. Non-profit applicants and any proposed subrecipient of a non-profit must provide documentation of non-profit and/or public status. Any of the following constitutes acceptable proof of non-profit status:

- 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.
- A copy of a currently valid IRS tax exemption certificate.
- A statement from a State taxing body, State attorney general, or other appropriate State official certifying that the applicant organization has a non-profit status and that none of the net earnings accrue to any private shareholders or individuals.
- A certified copy of the organization's certificate of incorporation or similar document that clearly establishes non-profit status.
- Any of the items in the subparagraphs immediately above for a State or national parent organization and a statement signed by the parent organization that the applicant organization is a local non-profit affiliate.
- In addition, DHS will not consider multiple applications from a single organization serving as the lead. If more than one application is submitted by a single organization as the lead, the later in time will be considered, unless the later application clearly indicates a unique role for that organization, other than as lead for this activity.

3. Other Eligibility Criteria (*If applicable*)

Non-Responsive Applications: An application will be deemed non-responsive and not considered for review if:

1. The budget request for the budget period exceeds the maximum of $549,996 (direct and indirect costs).

2. The Project Narrative exceeds 15 pages (Note: The page limit does not include any of the attachments or forms).
3. The Project Narrative does not include each of the specified headings in the order identified in Section D.
4. The Application does not include one or more of the required forms or documents listed under Section D. The required forms and documents are:

- Form SF-424 – Application for Federal Assistance
- Form SF-424A – Budget
- Form SF-424B – Assurances – Non-Construction Programs
- Certification Regarding Lobbying
- Budget Narrative and Table
- Project Abstract
- Project Narrative
- Project Plan
- Documentation of non-profit status

Applications rejected by Grants.gov for unregistered AOR will be disqualified and will not be considered for competition.

4. Cost Share or Match

No cost share is required

<u>Application and Submission Information</u>

1. Key Dates and Times

a. Application Start Date: *08/29/2022*

b. Application Submission Deadline: *09/07/2022 at 11:59:59 PM [Eastern Standard Time]*

c. Anticipated Funding Selection Date *(Optional)*: **No later than** *09/30/2022*

d. Anticipated Award Date *(Optional)*: **No later than** *09/15/2022*

e. Other Key Dates *(If applicable)*

Event	**Suggested Deadline for Completion**
Obtaining UEI Number	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	One week before actual submission deadline

2. Agreeing to Terms and Conditions of the Award

By submitting an application, 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.

For a hardcopy of the full NOFO, please write or fax a request to:

Stephanie Dawkins
Grants Officer
Office of Procurement Operations
245 Murray Lane, SW, Mail Stop 0115
Washington, D.C. 20528-0115
Stephanie.Dawkins@hq.dhs.gov
Phone: 202-774-9760

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. If you experience difficulties accessing information or have any questions, please call Grants.gov customer support at 1-800-518-4726.

4. **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. Apply for, update, or verify their unique entity identifier UEI Number and Employer ID Number (EIN)
b. In the application, provide a valid UEI number, which is currently the unique entity identifier;
c. Have an account with https://login.gov/;
d. Register for, update, or verify their SAM account and ensure the account is active before submitting the application.
e. Create a Grants.gov account.
f. Add a profile to a Grants.gov account.
g. Establish an Authorized Organizational Representative (AOR) in Grants.gov;
h. Submit (if applicable, add: an initial) application in Grants.gov;
i. (If applicable) Submit the final application in the <insert applicable system>; and
j. 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 UEI and 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.

5. **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. *If applicable, add:* For this funding opportunity, the *<DHS GRANT AND FINANCIAL ASSISTANCE DIVISION>* requires applicants to submit applications through Grants.gov.

6. **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 UEI Number, 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 UEI and SAM registrations 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.

1) *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 data entry field labeled "Organizational UEI" on the SF-424 form.

   For more detailed instructions for obtaining a UEI number, refer to: https://sam.gov/content/entity-registration.

2) *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.

   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.

3) *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.

4) *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.

5) *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.

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

7) *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.**

7. 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.

8. Timely Receipt Requirements and Proof of Timely Submission

a. *Online Submission.* All applications must be received by [INSERT TIME] Eastern time on the due date established for each program. 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.

b. *If the application is submitted initially through Grants.gov and then finalized in another system, use language like this:* As application submission is a two-step process, the applicant with the Authorized Organizational Representative (AOR) role who submitted the application will receive an acknowledgment of receipt, a tracking number (GRANTXXXXXXXX) from Grants.gov, and *[insert DHS GRANT AND FINANCIAL ASSISTANCE DIVISION's tracking number or information]* with the successful transmission of the initial application. This notification does not serve as proof of timely submission as the application is not complete until it is submitted in *[DHS GRANT AND FINANCIAL ASSISTANCE DIVISION's system]*. All applications must be received in *[DHS GRANT AND FINANCIAL ASSISTANCE DIVISION's system]* by **HH:MM AM/PM Eastern Time on *[Month Day, Year]*.** *If applicable, add how the applicant will know whether its final submission in DHS GRANT AND FINANCIAL ASSISTANCE DIVISION's system is successful & submitted on time, such as stating that there is an electronic date/time stamp generated in the system or that the applicant will receive an email to confirm receipt.*

9. Content and Form of Application Submission

Required Forms

Complete the required forms in accordance with the application instructions on Grants.gov. If submitting any information that is deemed proprietary, privileged, confidential, or financial, please denote the beginning and ending of such information with asterisks (*).

1. 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 form 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).

2. 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.

3. Certifications/Assurances: Applicants must submit:

a. Form SF-424B – Assurances – Non-Construction Programs; and
b. Certification Regarding Lobbying. If paragraph two of the certification applies, then complete and submit the SF-LLL Disclosure of Lobbying which is provided as an optional form in the application package.

By signing and submitting an application under this announcement, the applicant is providing: Certification Regarding Drug-Free Workplace Requirements (see Attachment B); Certification Regarding Debarment, Suspension, and Other Responsibility Matters – Primary Covered Transactions (see Attachment C); and Certification that the applicant is not delinquent on any federal debt.

Required Documents

4. **Budget Table and Narrative**: See also Restrictions on Use of Award Funds.

If a subrecipient is proposed under the project, applicants must provide a separate subrecipient budget narrative and table following the same format and with the same level of detail as that of the applicant (i.e., by Object Class Category/Cost Classification). Each subrecipient budget and supporting detail should be separate from the applicant's budget narrative.

If any fees are proposed that will result in program income, please show in the budget how this income will be used.

Budget Table
Provide your budget request in a table format. This must be provided either in the same document as the budget narrative or uploaded as a separate document under the "Other Attachments" form found under the "Optional Documents" section of the application package." Include all budget categories, as listed in the budget narrative section. Under each category, list the line items requested. See a sample table below.

Note: This sample table shows the Personnel category only. Applicants must provide information on all budget categories.

Budget Table	Year 1	Total	Category and Item	In-Kind	DHS	Total
In-kind	DHS	Total	1. Personnel-1 FTE	$X	$X	$X
$X	$X	$X	TOTAL Personnel	$X	$X	$X
$X	$X	$X				

Include costs for the performance year. Show a total of all requested federal grant funds. This total should match the total listed on the project abstract. Budget categories below should add up to this total. This total should not include any in-kind costs. The in-kind contribution (if applicable) total should be listed separately.

Provide budget information in the order listed below. Budget detail is required for:

a. **In-Kind Costs**: The dollar value of non-cash donations to the project. These donations may be in the form of space, supplies, salaries, etc. The costs should be calculated at the verifiable fair-market value.
b. **Personnel**: Costs of employee salaries and wages. For each staff person, provide the name (if known), title, time commitment to the project as a percentage of a full-time equivalent (FTE), annual salary, and grant funded salary. Do not include the costs of consultants. Consultants are to be included under "Contractual."
c. **Fringe Benefits**: Costs of employee fringe benefits unless treated as part of an approved indirect cost rate. Provide the method used to calculate the proposed rate amount. If a fringe benefit has been negotiated with, or approved by, a cognizant federal agency, provide a copy of the agreement. If no rate agreement exists, provide a breakdown of the amounts and percentages that comprise fringe benefit costs such as health insurance, FICA, retirement insurance, taxes, etc. Identify the base for allocating these fringe benefit expenses.
d. **Travel**: Costs of project-related travel by employees of the applicant organization (do not include costs of sub-contractor or consultant travel). For each proposed trip, provide the purpose, number of travelers, travel origin and destination, number of days, and a breakdown of costs for airfare, lodging, meals, car rental, and incidentals. The basis for the airfare, lodging, meals, car rental, and incidentals must be provided, such

as past trips, current quotations, Federal Travel Regulations, etc. Foreign travel is not permitted.

e. **Equipment**: Equipment costs are not anticipated under this NOFO.
f. **Supplies**: Costs of all tangible personal property. Specify general categories of supplies and their costs. Show computations and provide other information which supports the amount requested.
g. **Contractual**: Costs of all contracts for services and goods except for those that belong under other categories such as equipment, supplies, construction, etc. Include third party evaluation contracts (if applicable) and contracts with secondary recipient organizations. Demonstrate that all procurement transactions will be conducted in a manner to provide, to the maximum extent practical, open and free competition. Identify proposed sub- contractor work and the cost of each sub-contractor. Provide a detailed budget for each sub-contractor that is expected to perform work estimated to be $25,000 or more, or 50% of the total work effort, whichever is less.
    - Identify each planned subcontractor and its total proposed budget. Each subcontractor's budget and supporting detail should be included as part of the applicant's budget narrative.
    - Provide the following information for each planned subcontract: a brief description of the work to be subcontracted; the number of quotes solicited and received, if applicable; the cost or price analysis performed by the applicant; names and addresses of the subcontractors tentatively selected and the basis for their selection; e.g., unique capabilities (for sole source subcontracts), low bidder, delivery schedule, technical competence; type of contract and estimated cost and fee or profit; and, affiliation with the applicant, if any.
    - Recipient may be required to make pre-award review and procurement documents available to DHS, including request for proposals or invitations for bids, independent cost estimates, etc. This may include procurements expected to exceed the simplified acquisition threshold fixed at 41 USC 403(11) (currently set at $250,000) and expected to be awarded without competition or only one bid or offer is received in response to a solicitation.

    A. All required flow down provisions in the award must be included in any subcontract.
h. **Other Direct Costs**: Any other items proposed as direct costs. Provide an itemized list with costs and state the basis for each proposed item.
i. **Indirect Costs**: Provide a copy of the latest 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.
NOTE: If no indirect cost rate agreement is included, no indirect costs should be listed in the proposed budget.

5. **Project Abstract (3 single-spaced page maximum)**
Provide the information below in a separate document, suitable for public dissemination. The project abstract must not include any proprietary/confidential information. Attach the Project Abstract to the "Project Abstract" form within the application package.

General Information	
1.	**Organization Legal Name**
2.	**Organization Legal Address** (Number and street, city, state, zip code)
3.	**Head of the Organization** (Name, title, address, phone number, email
4.	**Authorized Official**, the person at the organization authorized to sign to receive
5.	**Grant Project Manager**, the person who will manage the operations of the grant project and will serve as CISA's primary point of contact (Name, title, address, phone number, email address)
6.	**Type of Organization** (e.g., community/faith-based organization, etc.)
7.	**Project Description** (200 words or less) Provide a one-paragraph summary of the following: □ The organization's experience providing cybersecurity awareness services and number of years providing services; □ A description of the constituency, that the organization will serve; and □ Proposed grant project activities and outcomes.
8.	**Total Federal Funding Requested** (Not to exceed $549,996)

9.	**Total Federal Funding Allocated for Cybersecurity Awareness Campaign Program Activities and Materials**
10.	**Total Federal Funding Allocated for Cybersecurity Awareness Month Activities and Materials**
11.	**Applicant's Total In-Kind Contributions** (if applicable)
12.	**Geographic Area/Community** where services will be provided
13.	**Congressional District** (based on the legal address of the applicant organization)
14.	**Targeted Communities** (if applicable)
15.	**Number of Full-Time Equivalents (FTEs)** Indicate the number of intended grant-funded FTEs. Include part-time work as percentages of FTEs. Include any grant-funded subrecipient FTEs.
16.	**Proposed Subrecipient Organization** (if applicable) (Organization name, point of contact name and title, address, phone number, email address)
17.	**Services Proposed by Subrecipient Organization**
18.	**Are all program sites in compliance with the Americans With Disabilities Act?**
19.	**Has your organization previously received a CISA grant?** If so, provide year(s)
Program Outcomes (for grant-funded services over the one -year period)	
20.	Increased cybersecurity awareness across stakeholder groups.
21.	Enhanced and newly developed materials for cybersecurity awareness.
22.	Successful events that promote cybersecurity across all media platforms.

6. **Project Narrative (15-page maximum)**

Use this section to provide a comprehensive description of the proposed program, addressing all required elements in response to the evaluation criteria. Items 6.a. – 6.c. below are the mandatory elements that must be included in the Project

Narrative. You must follow the order specified below, using the title headings provided below to identify each element.

Required Headings:

a. Problem Statement Describing the Need and Current State of Public Cybersecurity Awareness
b. Program Design and Rationale
c. Organizational Qualifications and Experience

An application that does not include each required element listed in the order provided in this section and/or is in excess of 15 double-spaced pages will be deemed non-responsive and will not be considered.

Format Requirements

- Include the title "Project Narrative" at the top of the first page.
- Ensure that the application can be printed on 8 ½" x 11" single-sided paper.
- Use double-spacing.
- Do not include any marks from the "Track Changes" tool in your word processing program.
- Font size must be at least 12 point, preferably Times New Roman font.
- Margins must be at least one (1) inch at the top, bottom, left and right of the paper.
- Project narrative pages must be numbered "1" of "XX."
- Pages should be numbered consecutively and are limited to a total of 15 pages.
- Attach the completed Project Narrative to the "Project Narrative Attachment" form.

Required Project Narrative Sections

a. Problem Statement Describing the Need and Current State of Public Cybersecurity Awareness: Use this section to demonstrate the current state and recommended focus areas of cybersecurity awareness among the general public; small/medium businesses; the academic community, including K-12 and higher education educators, administrators, and students; and/or other key stakeholders. Narratives should incorporate sound research and data to support the problem statement.

b. Program Design and Rationale: Provide a brief overview of your cyber security awareness program design that covers the following: 1) a description of the cyber security awareness strategy recommended to address the recommended focus areas; 2) how the proposed grant-funded

program will execute the recommended strategy; 3) how the program design will meet the stakeholders' issues; and 4) the anticipated outcomes of the program.
Provide a list of key personnel, at a minimum a project manager. For each provide a brief position description, the individual's qualifications and relevant training. Attach resumes for all key personnel. Note: Resumes do not count towards the project narrative page limit.

c. Organizational Qualifications and Experience: Use this section to demonstrate the organization's qualifications and experience to successfully manage and implement all aspects of the grant-funded project. Describe:
    - The organization's and, if applicable, sub-applicant's experience conducting cyber security awareness programs. Indicate dates and total years of experience. Describe program achievements.
    - The organization's experience measuring, tracking, evaluating, and reporting outcomes related to cyber security outreach and awareness.
    - The organization's management structure.
    - The organization's recent experience managing grant-funded programs and its fiscal management ability.
    - The applicant's relationship with any proposed subrecipient organization and how the applicant will manage the subrecipient. The applicant must include a Memorandum of Understanding (MOU) between the organizations as a required attachment to the grant application.

7. **Project Plan**
Provide a project plan in table format that outlines the applicant's planned activities and anticipated outcomes by quarter. The project plan should be attached to the "Other Attachments" form found under the "Optional Documents" section of the application package. Note: Applications that do not contain a project plan will be considered non-responsive and will not be scored.

Information should be provided for the performance period. For each quarter, provide the following information:

i. Planned activities, including staff hiring and training, outreach, data collection, etc. For each activity, provide the month(s) when the activity will take place and the staff responsible for each activity.
ii. Anticipated Outcomes.

8. **Documentation of Non-profit Status**
The applicant must provide documentation of non-profit status. Any of the following constitutes acceptable proof of non-profit status:

i. 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.
ii. A copy of a currently valid IRS tax exemption certificate.
iii. A statement of a State taxing body, State attorney general, or other appropriate State official certifying that the applicant organization has a non-profit status and that none of the net earnings accrue to any private shareholders or individuals.
iv. A certified copy of the organization's certificate of incorporation or similar document that clearly establishes non-profit status.
v. Any of the items in the subparagraphs immediately above for a State or national parent organization and a statement signed by the parent organization that the applicant organization is a local non-profit affiliate.
vi. A signed statement on official letterhead by an official authorized to apply for grant funds on behalf of the non-profit and/or public entity shall suffice.

The documentation of non-profit status should be attached to the "Attachments" form found under the "Mandatory Documents" section of the application package.

10. Other Submission Requirements

Attach the following items using the "Other Attachments" form found under the "Optional Documents" section of the application package.

a. Resumes of key personnel (one page each) or job descriptions for key positions if vacant.
b. If proposing a subrecipient who will provide additional or complementary grant-funded services, a draft [or final signed] Memorandum of Understanding (MOU) between the recipient and the subrecipient shall be included. The MOU should clearly describe the scope of work to be performed, roles, responsibilities, and agreed upon activities, including remuneration, and other terms and conditions that structure or define the relationship (e.g., in-kind services, dollars, staff, space, equipment, etc.). DHS reserves the right to contact all organizations listed in the application prior to making an award.
c. Current organizational chart that shows the leadership and staff structure.
d. Negotiated Fringe Benefit Agreements or, if no agreements exist, the amounts and percentages of all items that comprise the fringe rate, and the basis for allocation, if separate from the Indirect Cost Rate Agreement.
e. Indirect Cost Rate Agreements.
f. A list of other federal grant programs from which your organization currently receives funding or for which it has applied.

11. Intergovernmental Review *(Include if applicable)*

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*).

12. Funding Restrictions

The use of award funds is restricted to the activities of carrying out national cybersecurity awareness activities. These activities include:

- strategy development and measurement,
- communications materials production,
- stakeholder engagement and outreach,
- cross promotion of cybersecurity resources,
- Cybersecurity Awareness Month activities and
- program management.

13. Allowable Costs

1. DHS grant or 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 must be consistent with the statutory authority for the award. Grant or cooperative agreement funds and non-monetary support under this NOFO may not be used for cost-sharing or matching funds for other Federal grants, lobbying, or intervention in Federal regulatory or adjudicatory proceedings. In addition, Federal funds may not be used to sue the Federal government or any other government entity.

2. Equipment purchases.
   a. Prior to the purchase of equipment in the amount of $5,000 or more per unit cost, the Recipient must obtain the written approval from DHS.
   b. The Recipient shall maintain an annual inventory which will include a brief description of the item, serial number and amount of purchase for equipment purchased with grant/cooperative agreement funds, or received under a grant or cooperative agreement, and having a $5,000 or more per unit cost. The inventory must also identify the sub-award under which the equipment was purchased.
   c. Insurance on the equipment will be the responsibility of the Recipient.

   d. Disposition instructions" will be provided to the recipient within 120 days of closeout (the submission of the recipient's final reports). Equipment purchases are limited to those items that fall within the categories described in Attachment C, "Eligible Equipment."
   e. Pre-award costs are allowable only with the written consent of DHS and included in the award agreement.

3. **Ineligible Funding Purposes.** Grant funds under this NOFO may not be used for the following purposes:

a. Construction costs and purchase of real property.
b. Foreign Travel.
c. Funding for direct reimbursement of recipient's grant application development.
d. Costs for food or refreshments.
e. Incentive items or gift cards.
f. General volunteer stipends.
g. Living allowances for any volunteer service program participants.
h. Grant or cooperative agreement funds and non-monetary support may not be used for cost-sharing or matching funds for other Federal grants, lobbying, or intervention in Federal regulatory or adjudicatory proceedings.
i. Federal funds may not be used to sue the Federal government or any other government entity.

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

Management and Administrative Costs are allowable for the recipient and any proposed subrecipient (if applicable). For more information on allowable costs, please see Section D, Funding Restrictions and Section

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

Indirect Costs are allowable for the recipient and any proposed subrecipient (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.

D. Application Review Information

1. Application Evaluation Criteria

Prior to making a Federal award, the DHS Grants and Financial Assistance Division is required by 31 U.S.C. § 3321 note, 41 U.S.C. § 2313, and 2 C.F.R. § 200.205 to review information available through any OMB-designated repositories of governmentwide eligibility qualification or financial integrity information. Therefore, application evaluation criteria may include the following risk-based considerations of the applicant:

a. **Programmatic Criteria**

CISA program officials will be responsible for the evaluation of applications. The following criteria will be used to evaluate proposals. The total weight for all criteria equals 100 points for the Grant. Each criterion will be evaluated by the technical review team.

1. **Program Design and Rationale (35 points)**: The extent to which the applicant proposes a comprehensive program design to develop cybersecurity awareness programs, activities, campaigns, tools and resources. The extent to which the applicant can justify why the program design will form the basis of a successful and effective awareness program that will meet the cybersecurity education needs of the public and private sector and academia. The extent to which the applicant can show the relationship between the program design and anticipated outcomes. The extent to which the applicant demonstrates how the organization will effectively educate key stakeholder communities that will result in an empowered constituency regarding their online activity and to incorporate the Internet of things securely and safely, protecting themselves and the cyber infrastructure. The extent to which the applicant can convey innovative strategies and plans to reach unique stakeholder groups with targeted messaging around the greatest and most prevalent risks as well as existing, traditional stakeholders and partners. The extent to which applicant can provide methodology for measuring successful Campaign/National Cybersecurity Awareness Month (NCSAM) activity outcomes/impact by getting stakeholders to absorb messages from these activities and in others carrying Campaign/NCSAM messages on their own. Also, the extent to which provided metrics are aligned to the program objectives overall.
2. **Project Management and Organizational Capability (20 points)**: The degree to which the applicant has a sound management and fiscal structure including: well-defined roles for administrators and staff, established financial management systems, and a commitment to ongoing staff and volunteer development and training to ensure effective program implementation. The extent to which the applicant identifies and demonstrates that qualifications, capabilities, and educational background of the identified key personnel (at a minimum the Project

Manager) who will manage and implement the program are relevant and will contribute to the success of program goals and objectives.

3. **Demonstrated Experience and Past Performance (25 points)**: The extent to which the applicant demonstrates current (or recent past performance) successful and effective development and leadership of initiatives to generate awareness among users; small/medium-sized businesses; the academic community; and other stakeholders. The extent to which the applicant has experience managing grant-funded programs. The extent to which the applicant has experience establishing a baseline about the current situation with respect to key stakeholders and issues and has experience measuring effectiveness of efforts and progress over time. The extent to which the applicant has a track record of successfully promoting awareness. The extent to which the applicant has established relationships with partner and stakeholder organizations. The depth of the applicant's experience in working as a neutral third party and spokesperson to coordinate activities with multiple entities.
4. **Project Plan and Budget (20 points)**: The extent to which the applicant explains each element of the project phases and provides milestones that are well defined and can realistically be completed within the grant cycle. The extent to which the applicant clearly defines performance standards and provides a plan to track, report, and evaluate performance outcomes. The extent to which the applicant can correlate and support the program's budget to the project phases and implementation timeline. The extent to which administrative/management costs are balanced with funds designated for the provision of campaign planning, media strategy and outreach.

b. **Financial Integrity Criteria**

Prior to making a federal award, the <*DHS GRANT AND FINANCIAL ASSISTANCE DIVISION*> is required by 31 U.S.C. §3321 note, 41 U.S.C. §2313, and 2 C.F.R. §200.205 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:

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.

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):

1) *<DHS GRANT 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.
2) An applicant, at its option, may review information in FAPIIS and comment on any information about itself that a federal awarding agency previously entered.
3) *<DHS GRANT 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

DHS will conduct an initial review of applications to determine the responsiveness of the application. If an applicant is determined to be ineligible or an application is determined to be non-responsive, DHS will notify the applicant. All responsive applications will be reviewed as described below:

1. DHS will assemble subject matter experts from inside of the Federal Government to review the full proposal. Reviews of submitted applications will be conducted either on site or by remote review.
2. At a minimum, 2 subject matter experts will review the proposal and provide summary comments based on the published criteria. The reviewers will assign a score and provide summary comments based on the published evaluation criteria. DHS/CISA staff will conduct a post review quality control or scores and comments to ensure that every eligible application receives full and fair consideration.
3. DHS designated Selection Authority (SA) will make a final funding decision based upon the results of the evaluation, and the overall goals of the Cybersecurity Awareness Program.
4. DHS may perform additional reviews of the applicant organization and any subrecipients and/or its key personnel. This may include publicly available materials and/or government databases and may have a bearing on award outcome.
5. After the technical review and before making a final funding decision, DHS may contact the highest-ranking applications to seek clarification and to negotiate technical and programmatic aspects of the application. If an application includes a subrecipient that will provide additional or complementary grant-funded services in partnership with the main applicant, DHS may request to speak with all parties included in the application to ensure enough planning and coordination has taken place prior to making an award.

6. Confidentiality and Conflict of Interest: Technical and cost proposals submitted under this funding opportunity will be protected from unauthorized disclosure in accordance with applicable laws, and regulations. DHS may use one or more support contractors in the logistical processing of proposals. However, proposal selection and award decisions are solely the responsibility of DHS personnel.
7. DHS discourages, and will not consider, any materials submitted by or on behalf of the applicant (i.e., letters of support) other than those materials requested in this funding opportunity announcement.

E. 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.**
This section must address what a successful applicant can expect to receive from the awarding office after a selection has been made.

The successful applicant can expect to receive a grant executed by a DHS Grant Officer authorized to obligate DHS funding. The award notice will be sent via email.

Notice of Not Selection for Award
Applications that were not selected for award will be notified by a Grants Officer via e-mail in a timely manner. If requested, applicants may send a written request to receive a written summary of reviewer comments related to each of the evaluation criteria, along with the points awarded to the application for each of the evaluation criteria within 60 days. The feedback comments will not include the identities of the panelists and reviewers.

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. In addition, awardees are required to comply with the prohibitions on certain telecommunications equipment and services under Section 889 of the John. S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019.

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.

Before accepting the award the AOR should carefully read the award package for 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.

The recipient and any sub-recipients must, in addition to the assurances made as part of the application, comply and require each of its subrecipient, contractors and subcontractors employed in the completion of the project to comply with all applicable statutes, regulations, executive orders, Office of Management and Budget (OMB) circulars, terms and conditions of the award, and the approved application.

Data Rights

General Requirements: Pursuant to 2 C.F.R. § 200.315*, Intangible Property*, DHS/CISA reserves a royalty free, non-exclusive and irrevocable right to reproduce, display, distribute copies, perform, disseminate, or prepare derivative works, or otherwise use the work, and to authorize others to do so, for Federal purposes in:

a. Any data that is first produced under this Agreement and provided to the Government; or
b. Any data owned by third parties that is incorporated in data provided to the Government under this Agreement.

"Data" means recorded information, regardless of form or the media on which it may be recorded.

Requirements for subawards: The Recipient agrees to include in any subaward made under this Agreement the requirements of the Copyright and Data Rights paragraphs of this article and of 37 C.F.R. 401.14.

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:

1. 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.

2. Final Federal Financial Report (SF-425) must be submitted to the DHS Grants Officer within 120 days after the expiration date of the Period of Performance. The final report shall be submitted via the Grants Solution System.

3. 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**
Program-specific reporting requirements have been included in Project Milestones under Section 1, Funding Opportunity Description and include the following:

1. Quarterly Performance Reports must be submitted to the DHS Grants Officer within 30 days after the end of each quarter. Reports shall be submitted as a grant note via the Grants Solution System.

3. Final Performance Report must be submitted to the DHS Grants Officer within 120 days after the expiration date of the Period of Performance. The final performance report shall include cumulative quantitative data, program accomplishments and challenges, and any promising practices related to cybersecurity awareness building. The final report shall be submitted as a grant note via the Grants Solution System.

c. **Additional Performance Reporting Requirements** *(if applicable)*

Report	**Estimated Deadline**
National Cybersecurity Awareness Program Plan	30 days after award
Program Quarterly Status Report on scope of effort and additional reporting as requested	Quarterly; 30 business days after the last day of each quarter
Program Monthly Status Meeting	Monthly
National Cybersecurity Awareness Month Program Tactical Plan	120 days prior to each NCSAM
Report of key outcomes from National Cybersecurity Awareness Month	30-45 days following conclusion of Awareness Month
Annual report to CISA of all activities related to the national awareness campaign to include recommendations on next steps. DHS will review the annual report and determine if there are additional tasks for the recipient.	Annually (based on fiscal year)

External Evaluation

Subject to availability of funding, DHS may conduct a formal evaluation of the Cybersecurity Awareness Program. As part of any formal program evaluation, grant recipients must permit DHS, upon reasonable notice, to review grant-related records and to interview the organization's staff regarding the program, and to respond in a timely and accurate manner to DHS requests for information relating to their grant program.

CISA Requests

Grant recipients may be asked periodically to review CISA public educational tools and materials and provide feedback as requested.

d. **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:

1) The final request for payment, if applicable;
2) The final FFR (SF-425).
3) The final progress report detailing all accomplishments;
4) A qualitative narrative summary of the impact of those accomplishments throughout the period of performance; and
5) Other documents required by this NOFO, terms and conditions of the award, or other <*DHS GRANT AND FINANCIAL ASSISTANCE DIVISION*> guidance.

If applicable, an inventory of all construction projects that used funds from this program must be reported with the final progress report.

After these reports have been reviewed and approved by <*DHS GRANT 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, Retention Requirements for Records.

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, Closeout. 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 GRANT 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.

e. **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 into a grant award with <*DHS GRANT AND FINANCIAL ASSISTANCE DIVISION*>, the recipient must notify <*DHS GRANT 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:

1) Are presently excluded or disqualified;
2) 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;
3) 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); or
4) 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 GRANT AND FINANCIAL ASSISTANCE DIVISION*> in accordance with 2 C.F.R. § 180.350.

f. **Reporting of Matters Related to Recipient Integrity and Performance** *(if applicable)*

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 of time 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.

ii. Monitoring and Oversight

Per 2 C.F.R. §200.329, <*DHS GRANT 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 GRANT 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 GRANT 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 GRANT AND FINANCIAL ASSISTANCE DIVISION*> requests for information relating to the grant program**.**

iii. 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 grant 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) for six months after the period of performance.

F. <u>DHS Awarding Agency Contact Information</u>

1. Contact and Resource Information

a. Contact and Resource Information

Please contact the following with technical questions during the hours of Mon-Fri, 9:00am-4:00pm EST:

The **Program Officer** is the DHS staff member responsible for monitoring the completion of work and technical performance of the projects or activities described in the Program Narrative Statement.

Justin Covington

Stakeholder Engagement Division (SED), Awareness and Outreach Branch
Cybersecurity and Infrastructure Security Agency
Desk: 703-603-5021 | Mobile: 202-815-4622
Email: Justin.Covington@cisa.dhs.gov

Mailing Address: CISA – NGR STOP 0645
Cybersecurity and Infrastructure Security Agency
1110 N. Glebe Rd.
Arlington, VA 20598-0645

Current Website Address: https://www.dhs.gov/stopthinkconnect

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

Stephanie Dawkins
Grant Officer
Office of Procurement Operations (MGMT OPO)
Phone: (202) 774-9760
Email: Stephanie.dawkins@hq.dhs.gov

Mailing Address: 245 Murray Ln., SW
Mail Stop: 0115, Rm 3051
Washington, D.C. 20528-0115

G. Additional Information

a. **Period of Performance Extensions**

Extensions to the period of performance under this program are allowed.

1. **Extensions**
   Applicants may request a no-cost extension in order to complete all project activities. The request must be submitted in writing 60-days prior to the expiration of the performance period. The written request shall outline the reason(s) for the extension along with the proposed new expiration date. Requests for extensions to the period of performance are subject to approval by DHS and can only be authorized in writing by the DHS Grant Officer.

2. **Prior Approval**
   The Recipient shall not, without the prior written approval of DHS, request reimbursement, incur costs or obligate funds for any purpose pertaining to the

operation of the project, program, or activities prior to the approved Budget Period.

3. **Budget Revisions**
   a. Transfers of funds between direct cost categories in the approved budget when such cumulative transfers among those direct cost categories exceed ten percent of the total budget approved in this Award require prior written approval by the DHS Grants Officer.
   b. The Recipient shall obtain prior written approval from the DHS Grants Officer for any budget revision that would result in the need for additional resources/funds.
   c. The Recipient is not authorized at any time to transfer amounts budgeted for direct costs to the indirect costs line item or vice versa, without prior written approval of the DHS Grants Officer.

4. **Post-award Program Income**
   In the event program income becomes available to the recipient post-award, it is the recipient's responsibility to notify the DHS Grants Officer to explain how that development occurred, as part of their request for guidance and/or approval. The Grants Officer will review approval requests for program income on a case-by-case basis; approval is not automatic. Consistent with the policy and processes outlined in 2 C.F.R. Part 200, pertinent guidance and options, as determined by the type of recipient and circumstances involved, may be approved by the Grant Officer. If approval is granted, an award modification will be issued with an explanatory note in the remarks section of the face page concerning guidance and/or options pertaining to the recipient's approved request. All instances of program income shall be listed in the progress and financial reports

a. 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 based on 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), UEI 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.

Applicant Disclosure of High-Risk Status

Applicants are to disclose if they are currently designated as high risk by a federal awarding agency. This includes, but is not limited to, any status requiring additional oversight by a federal awarding agency due to past programmatic, administrative or financial concerns. If an applicant is designated as high risk by a federal awarding agency, it should provide an explanation with the application package and include the following information:

- The federal awarding agency that assigned the high-risk status;
- The federal awarding agency's point of contact for the risk status, including name, phone number and email address;
- Date of the risk status designation;
- Reason(s) for the risk status.

DHS seeks this information to ensure appropriate federal oversight of all grant awards. The disclosure of an organization's risk status does not disqualify it from receiving an award; however additional grant oversight may be required. If necessary, this information will be provided in the award documentation. Failure to disclose high risk status may result in award termination or other remedies.