

The Department of Homeland Security (DHS)

Notice of Funding Opportunity (NOFO)

FY'23 Cybersecurity Awareness Campaign

Contents

A. Program Description	4
1. Issued By.....	4
2. Assistance Listings Number.....	4
3. Assistance Listings Title	4
4. Funding Opportunity Title	4
5. Funding Opportunity Number.....	4
6. Authorizing Authority for Program	4
7. Appropriation Authority for Program	4
8. Announcement Type.....	4
9. Program Category (Optional).....	5
10. Program Overview, Priorities, Goals, Objectives, and Tasks	5
11. Performance Measures	9
B. Federal Award Information.....	10
1. Available Funding for the NOFO: \$549,996.00	10
2. Projected Number of Awards (Optional): One (1).....	10
3. Period of Performance: 29 Months	10
4. Projected Period of Performance Start Date(s): 9/30/2023.....	10
5. Projected Period of Performance End Date(s): 2/28/2026	10
6. Initial Budget Period: 9/30/2023 to 9/29/2024.....	10
Budget Period 29/30/2024 to 9/29/2025	10
Budget period 39/30/2025 to 2/28/2026	10
7. Funding Instrument Type: Cooperative Agreement	11
C. Eligibility Information	12
1. Eligible Applicants.....	12
2. Applicant Eligibility Criteria	12
3. Other Requirements	12
4. Other Eligibility Criteria/Restrictions (If applicable)	12
5. Cost Share or Match.....	13
D. Application and Submission Information	13
1. Key Dates and Times	13
2. Agreeing to Terms and Conditions of the Award	13
3. Address to Request Application Package	13
4. Unique entity identifier and System for Award Management (SAM)	14

5. Steps Required to Submit an Application, Unique Entity Identifier, and System for Award Management (SAM)	14
6. Electronic Delivery	15
7. How to Register to Apply through Grants.gov	15
8. How to submit an Application to DHS via Grants.gov	16
9. Timely Receipt Requirements and Proof of Timely Submission.....	17
10. Content and Form of Application Submission.....	18
11. Other Submission Requirements.....	23
E. Application Review Information	25
1. Application Evaluation Criteria	25
2. Review and Selection Process.....	27
F. Federal Award Administration Information.....	28
1. Notice of Award.....	28
2. Notice of Not Selection for Award	28
3. Administrative and National Policy Requirements.....	28
4. Reporting.....	28
5. DHS Awarding Agency Contact Information.....	32
6. Other Information	32

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. Information about requesting a UEI 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>.

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 Listings Number**
97.128
3. **Assistance Listings Title**
Cybersecurity Awareness Campaign
4. **Funding Opportunity Title**
Cybersecurity Awareness Campaign
5. **Funding Opportunity Number**
DHS-23-CISA-128-CSA001
6. **Authorizing Authority for Program**
Homeland Security Act of 2002, Pub. L. No. 107-296, § 102(b)(2) (codified as amended at 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 Appropriation Act, 2023, Title III Protection, Preparedness, Response, and Recovery, Cybersecurity and Infrastructure Security Agency
8. **Announcement Type**
Initial, Year 1

9. **Program Category**

N/A

10. **Program Overview, Priorities, Goals, Objectives, and Tasks**

a. **Overview**

As America's Cyber Defense Agency, CISA leads the national effort to understand, manage, and reduce risk to our critical infrastructure from both cyber and physical threats.

Our nation faces unprecedented cybersecurity risks that can affect our day-to-day lives, economy, and national security. In alignment with the [Department of Homeland Security's Strategic Plan for Fiscal Years 2020-2024 | Homeland Security \(dhs.gov\)](https://www.dhs.gov/strategic-plan), it is essential to prepare for and protect against these risks, and we must also provide awareness concerning the importance of safeguarding our Nation's critical infrastructure from malicious cyber activity and how individuals can secure their sensitive data and stay safe online.

The primary focus of the FY 2023 Cybersecurity Awareness Campaign (the Campaign) is to provide awareness to the Nation concerning cybersecurity risks and provide messaging, tools, and resources that encourage the American public, business and industry to reduce their exposure to online risks and malicious actors. Through strategies both implemented during Cybersecurity Awareness Month in October, and encouraged throughout the year, the campaign seeks to improve the public's understanding of cyber threats as well as amplify opportunities Americans can leverage to strengthen their own cybersecurity posture and encourage year-round discussion, engagement, and actions we must all take every day to reduce cyber risk to ourselves and those we care about.

The campaign aligns with the Department of Homeland Security Strategic Plan for 2020-2024 by supporting Goal 3: Security Cyberspace and Critical Infrastructure and Goal 5: Strengthen Preparedness and Resilience. Additionally, it also aligns to the 2023-2025 CISA Strategic Plan by supporting Goal 2: Risk Reduction and Resilience and Goal 3: Operational Collaboration.

The Cybersecurity Awareness Campaign serves to further the Administration's National Cybersecurity Strategy that builds on the work in support of Executive Order 14028 (Improving the Nation's Cybersecurity) and National Security Memorandum 5 (Improving Cybersecurity for Critical Infrastructure Control Systems), among other efforts and initiatives; and support the National Security Strategy's vision of unprecedented government collaboration with civil society, private industry, and our international allies and partners.

Through implementation of the CISA Strategic Plan (2023-2025), (<https://www.cisa.gov/resources-tools/resources/2023-2025-strategic-plan>), CISA is working to ensure that the cyber and physical infrastructure that Americans rely on every hour of every day is safe, secure, and resilient, and through Strategic Plan, Goal 2, we reduce risks to, and strengthen resilience of, America's critical infrastructure.

Consistent with the Strategic Plan, Cybersecurity Awareness Month, held annually in October, supports our strategic goals to: ensure the cyber defense of the Nation by helping to spearhead the national effort to ensure defense and resilience of cyberspace; encourage efforts to reduce risks to, and strengthen resilience of, America's critical infrastructure; and help strengthen whole-of-nation operational collaboration and information sharing, especially

through our efforts to optimize collaborative planning and implementation of stakeholder engagements and partnership activities, streamlining stakeholder access to and use of appropriate CISA programs, products, and services, and enhance information sharing with CISA's partnership base.

b. Goals and Objectives

- **Goals**

This cooperative agreement supports the CISA Cybersecurity Awareness Campaign of which Cybersecurity Awareness Month held annually during October, is a focal point of the messaging and activities to accomplish the following Goals and encourage year-round actions to reduce such risks:

- i. Goal 1: Strengthen the security and resilience of critical infrastructure.
- ii. Goal 2: Assess and counter evolving cybersecurity risks through actions that promote threat risk reduction.
- iii. Goal 3: Build a national culture of preparedness for all Americans, ensuring equity and accessibility in our efforts to increase online and digital safety.
- iv. Goal 4: Build stakeholder relationships that encourage and support data-driven actions by governments, the private sector, tribes, non-profits, and the public that reduce cybersecurity risk.
- v. Goal 5: Reinforce the importance of secure by default and secure by design industry practices that do not place the first line of cyber threat risk reduction on those with the least capabilities and resources.
- vi. Goal 6: Encourage activities supported by data which result in key behavior change that reduce cyber risk.

October 2023, marks the 20th Cybersecurity Awareness Month and the campaign will execute a research and data-driven strategy that supports implementation of specific programs, activities, and outreach efforts that encourage year-round changes in behaviors that reduce cyber risk, and that are supported through messaging, materials and products throughout both Cybersecurity Awareness Month and throughout the year.

- **Objectives**

The following objectives will support the goals of the Cybersecurity Awareness Campaign:

- i. Objective 1: Educate the public, small businesses, and industry about the dangers of cyber threats and key actions that can be taken to mitigate risks.
- ii. Objective 2: Promote sustainable cybersecurity and encourage the technology industry to provide secure-by-default technology products with strong security features right out of the box, without added costs; and technology that is secure-by-design, purposefully developed, built, and tested to significantly reduce the number of exploitable flaws before they are introduced into the market for broad use.
- iii. Objective 3: Identify effective approaches to increase cybersecurity awareness among the general public and target audiences, including vulnerable populations and those with disabilities that may make it challenging to take actions that reduce risk.

- iv. Objective 4: Build relationships and coalitions across cybersecurity stakeholders to support Cybersecurity Awareness Month.
- v. Objective 5: Develop a baseline from which we can begin to measure the impact Cybersecurity Awareness Month campaign strategies and messaging has on changing behavior, increasing public awareness of cybersecurity risk.
- vi. Objective 6: Contribute to the agency's efforts to build a culture of preparedness, by 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.

c. Tasks

- 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 Campaign (the Campaign), culminating in Cybersecurity Awareness Month in October, to address cybersecurity risk most effectively. Further promote an annual Cybersecurity Awareness Campaign, that includes development of a coordinated strategy to engage partners and raise the visibility of CISA's Cybersecurity Awareness Month (October), to include tailored activities for specific audiences.
 - Measure, analyze and report on the effectiveness of awareness efforts and associated outcomes, to include:
 - Developing a methodology for measuring the Campaign's Cybersecurity Awareness Month outreach and outcomes.
 - Establishing baselines for awareness and actions associated with the Campaign's Cybersecurity Awareness Month
 - Conduct research to measure behavior changes due to the Cybersecurity Awareness Month exposure/saturation to determine program effectiveness and measurement of project, group and/or individual activities that encourage cybersecurity risk reduction actions by the targeted audiences so they might be used throughout the year. 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
 - Analysis and identification of activities that encourage cyber risk reduction by targeted audiences
 - Viable applicants must ensure they address capabilities and approach to driving behavior change among wide-ranging audiences. 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 that can be launched for cybersecurity awareness month and used throughout the year.

- Develop and execute creative website content and additional communication mediums for dissemination and promotion of cybersecurity messaging.
- Develop and execute digital content and additional communication mediums for dissemination and promotion of cybersecurity messaging, ensuring complete alignment within and produce visually engaging, action oriented and outcome driven cybersecurity awareness collateral applicable for launch during cybersecurity awareness month and can be utilized year-round.
- Stakeholder Engagement and Outreach
 - Development of an all-encompassing engagement strategy to include stakeholder and partnership mapping, engagement campaign planning and execution of activities undertaken during the Campaign's Cybersecurity Awareness Month seeking to increase awareness and utilization of CISA's products and services, through CISA's integration of public and private sector considerations, requirements, and objectives in mission planning.
 - Establish formal and informal partnerships with key cybersecurity stakeholder groups to reach target audiences and communities, which includes facilitating both new and improved partnerships, to execute a comprehensive Cybersecurity Awareness Campaign reaching across a wide range of audiences and communications channels during Cybersecurity Awareness Month.
 - Develop a coordinated messaging effort with public and private sector partners.
 - Establish and maintain a professional partnership and engagement tracking mechanism, which is accessible and developed in coordination with CISA's Cybersecurity Awareness Campaign team
 - 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, tribal, non-profit, and public and private sectors. This includes how the recipient will coordinate with existing cybersecurity awareness work being conducted by CISA and other federal agencies.
- Cross-promotion of Cybersecurity Resources
 - Utilize, incorporate, and promote DHS/CISA cybersecurity programs/resources wherever applicable and relevant.
 - Align awareness/outreach efforts to the CISA Strategic Plan, CISA/SED Stakeholder Engagement Plan, CISA's new Public Awareness Program, and CISA messaging, for long-term success, and create new and innovative ideas, content, and strategies for the Campaign's Cybersecurity Awareness Month that can be utilized throughout the year.
- Execute Cybersecurity Awareness Month Activities
 - Secure and conduct media engagement to promote Cybersecurity Awareness Campaign, and associated, available resources, to increase cybersecurity actions amongst the general public and target segments.
 - 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).

- Create, produce, and disseminate the Campaign’s Cybersecurity Awareness Month 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.
 - In coordination with CISA, develop an after-action report that identifies successes, highlights key metrics of the campaign, lessons-learned and best-practices, and areas to build on for future years, draft to be delivered by November 30, following Cybersecurity Awareness Month.
 - In coordination with CISA, provide the number, a list for, and all points of contact for all stakeholders by partner type, who participate in the Campaign’s Cybersecurity Awareness Month.
 - In coordination with CISA provide a list and examples of all material, posts, key messages, and other external facing materials in support of cybersecurity awareness month.

11. **Performance Measures**

The recipient will show the impact of its Cybersecurity Awareness Campaign activities through collection, measurement, tracking and reporting of key metrics that provide feedback on the breadth of the campaign’s outreach and efforts made by the recipient to meet the goals and objectives of the cooperative agreement. Reporting must be through cumulative year-end datasheet reporting of the following performance metrics:

- a. Strengthen the security and resilience of critical infrastructure
 - 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.
 - Types of Cybersecurity Awareness Campaign outreach engagements/instances targeted toward the critical infrastructure security stakeholder audience.
 - 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.
- b. Assess and counter evolving cybersecurity risks
 - Number Cybersecurity Awareness Campaign key messages offered related to reducing cybersecurity risks.
 - Actual or estimated number and demographics of community stakeholder groups reached through each type of outreach engagement/instance sorted by CISA Region, Federal State, Local, Tribal, Territorial, Non-Profits, Private Sector, and International Affiliation.
 - Number Cybersecurity Awareness Campaign key messages offered related to sustainable cybersecurity and for the technology industry to provide secure-by-default technology products and technology that is secure-by-design.

- c. Assess support of efforts to build a national culture of preparedness
 - Number of Cybersecurity Awareness Campaign key communications related to general public.
 - Number of Cybersecurity Awareness Campaign key communications products provided to general public by type/medium.
 - Research effort and types of Cybersecurity Awareness Campaign measurement tools used to measure changes in behavior toward cybersecurity.
 - Percent increase of social media activities in Q1 FY '24 over Q4 FY '23, amplifying cyber risk reduction activities and messaging from cybersecurity awareness month.
 - Estimated number and demographic of partners and 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 partnerships formed through Cybersecurity Awareness Campaign activities.
 - 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.
- d. Provide metrics to determine the effectiveness of the awareness campaign messaging efforts, including but not limited to:
 - Impressions
 - Customer engagement
 - Reach and frequency
 - Social reach for CISA's social media channels
 - Traditional Media placement and audience
 - Reputation
 - Search and interest volume
 - Site traffic

B. Federal Award Information

1. Available Funding for the NOFO:	\$549,996.00
2. Projected Number of Awards:	One (1)
3. Period of Performance:	29 Months
An extension to the period of performance is allowable. Refer to Section 6.	
4. Projected Period of Performance Start Date(s):	9/30/2023
5. Projected Period of Performance End Date(s):	2/28/2026
6. Initial Budget Period:	9/30/2023 to 9/29/2024
Budget Period 2	9/30/2024 to 9/29/2025
Budget period 3	9/30/2025 to 2/28/2026

- There will be up to three budget periods for the Federal Award, which are the following: 9/30/2023 to 9/29/2024; 9/30/2024 to 9/29/2025; and 9/30/2025 to 2/28/2026.
- The available funding for the NOFO described above is for the initial 12-month budget period from 9/30/2023 to 9/29/2024.
- Funding for non-competitive renewal awards for the second and third budget periods is conditioned on the availability of funds, satisfactory performance by the recipient, program authority, compliance with the terms and conditions of the Federal Award, and a DHS/CISA determination that continued funding is in the best interests of the federal government.
- A recipient may only carry forward unobligated balances from one budget period to a subsequent budget period with prior written approval of DHS/CISA

7. Funding Instrument Type:

Cooperative Agreement

DHS/CISA will exercise substantial programmatic involvement in the federal award through collaboration, participation, and other involvement in activities performed by the recipient in carrying out the scope of work. This will include the following:

- a. CISA will facilitate the recipient'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.
- b. 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 the Campaign's Cybersecurity Awareness Month events, as requested by the recipient. CISA will coordinate with the applicant as necessary on such participation.
- c. CISA must review and approve project materials before the recipient disseminates the materials, including:
 - Publications, brochures, presentation materials, products, documents, websites (or portions thereof), social media presence and activities, or other cybersecurity awareness collateral produced under this award 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 and approval.
 - Agendas for meetings, seminars, workshops, and conferences. Forty-five (45) days prior to the event, the recipient must submit draft agendas and handouts to the DHS Program Officer for review and approval.
- d. 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 must seek the DHS Program Officer's review and approval of its participation.
- e. The recipient must notify the DHS 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 the federal award.

C. Eligibility Information

1. Eligible Applicants

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.

2. Applicant Eligibility Criteria

Applicants whose mission is dedicated to promoting cybersecurity-related awareness and safe behavior online, and any proposed subrecipient, must provide documentation of non-profit status and tax exemption under Section 501(c)(3). 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.

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 Requirements

- **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.
- **Application relevance.** Applications that do not address the purpose of this announcement will not be considered.
- **Compliance and completeness.** Applications must substantially comply with the application submission instructions and requirements in this announcement, or they will not be considered.
- **Funding limits.** Applications with a budget exceeding the available federal funding will not be considered.

4. Other Eligibility Criteria/Restrictions (If applicable)

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

- a. The budget request for the initial budget period exceeds the maximum of \$549,996 (direct and indirect costs), unless the applicant is voluntarily contributing non-federal funding.
- b. The Project Narrative exceeds 15 pages (Note: The page limit does not include any of the attachments or forms).
- c. The Project Narrative does not include each of the specified headings in the order identified in Section D.
- d. 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
 - Project Abstract
 - Project Narrative
 - Project Plan
 - Documentation of 501(c)(3) non-profit status
- e. Applications rejected by Grants.gov for unregistered AOR will be disqualified and will not be considered for competition.

5. Cost Share or Match

There is no non-federal cost-share or matching requirement under the cooperative agreement. An applicant may pledge voluntarily committed cost-sharing in its proposed budget for the application, although voluntary cost-sharing will play no role in DHS/CISA's selection process. If DHS/CISA accepts the voluntary cost-sharing when issuing the Federal Award, the voluntary cost-share becomes a binding obligation.

D. Application and Submission Information

1. Key Dates and Times

Application Start Date: 07/03/2023

a. Application Submission Deadline: 08/03/2023 at 11:59:59 PM
Eastern Daylight Time

All applications must be received by the established deadline.

- b. Anticipated Funding Selection Date: 09/15/2023
 c. Anticipated Award Date: 09/30/2023
 d. Other Key Dates (If applicable)

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 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

Applications must be submitted in electronic format only. 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 Assistance Listing (formerly 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 email a request to:

Lisa Johnson
Lisa.Johnson1@hq.dhs.gov

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. 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>.

- 1) 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>.

- 2) 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>.
- 3) 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>.

- 4) 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>.

- 5) 5) Track Role Status: To track your role request, refer to: <https://www.grants.gov/web/grants/applicants/registration/track-role-status.html>.
- 6) 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 11:59:59 PM EDT 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.

10. 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 for the initial budget period 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 Narrative: See also Restrictions on Use of Award Funds.

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				

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.

The Budget Narrative describes costs associated with each object class category in the SF-424A and must include the following information.

- 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 salary allocated to the federal award. Do not include the costs of consultants. Consultants are to be included under “Contractual.”
- 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 rate has been negotiated with, or approved by, a cognizant federal agency for indirect costs, provide a copy of the fringe benefit rate agreement. If no fringe benefit 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.

- c. Travel: Costs of federal award-related travel by employees of the applicant organization (do not include costs of 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 meals, car rental, and incidentals must be provided, such as past trips, current quotations, Federal Travel Regulations, etc. Foreign travel is not permitted.
- d. Equipment: Equipment costs are not allowed.
- e. Supplies: Costs of all tangible personal property other than equipment. Specify general categories of supplies and their costs. Show computations and provide other information which supports the amount requested.
- f. Contractual: Costs of all contracts for services and goods except for those that belong under other object class categories. Include third party evaluation contracts (if applicable) and contracts with secondary recipient organizations. Identify proposed contractor work and the cost of each contractor. This will also include all costs for any subawards.
- g. Upon award, the recipient must provide a detailed budget for each 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 contractor and its total proposed budget. Each contractor's budget and supporting detail should be included as part of the applicant's budget narrative.
 - Provide the following information for each planned contract: a brief description of the work to be contracted; the number of quotes solicited and received, if applicable; the cost or price analysis performed by the applicant; names and addresses of the contractors 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 in accordance with 2 C.F.R. § 200.325.
 - All required contract clauses must be included in any contract.
- h. If a subrecipient is proposed under the federal award, 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.
- 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: Indirect costs are allowable under this program as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414 and Appendix IV (Indirect (F&A) Costs Identification and Assignment, and Rate Determination for Nonprofit Organizations). Applicants with a current negotiated indirect cost rate agreement that desire to charge indirect costs to a federal award must provide a copy of their negotiated indirect cost rate agreement at the time of application. Except as provided in 2 C.F.R. § 200.414(e), a nonprofit organization applicant that has not previously established an indirect cost rate seeking to charge indirect costs to the award must submit its initial direct cost proposal to the cognizant agency for indirect costs immediately after the organization is advised that a federal award will be made and, in no event, later than three months after the effective

date of the federal award. If DHS is not the applicant's cognizant federal agency for indirect costs, the applicant must provide DHS with a copy of its submitted proposal and the final negotiated indirect cost rate agreement. The regulation at 2 C.F.R. § 200.414(e) provides that any nonprofit organization applicant that has never received a negotiated indirect cost rate may elect to charge a de minimis rate of 10% of modified total direct costs (MTDC) which may be used indefinitely.

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 the agreement
5.	Cooperative Agreement Project Manager, the person who will manage the operations of the cooperative agreement and will serve as CISA's primary point of contact (Name, title, address, phone number, email address)
6.	Type of Organization
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 cooperative agreement project activities and outcomes.
8.	Total Federal Funding Requested (Not to exceed \$549,996.00)
9.	Total Federal Funding Allocated the Cybersecurity Awareness Campaign Activities and Materials for Cybersecurity Awareness Month
10.	Geographic Area/Community where services will be provided
11.	Congressional District (based on the legal address of the applicant organization)
12.	Targeted Communities (if applicable)
13.	Number of Full-Time Equivalents (FTEs) Indicate the number of intended cooperative agreement-funded FTEs. Include part-time work as percentages of FTEs. Include any cooperative agreement-funded subrecipient FTEs.
14.	Proposed Subrecipient Organization (if applicable) (Organization name, point of contact name and title, address, phone number, email address)
15.	Work Performed by Subrecipient Organization (applicants must include how their mission is dedicated to promoting cybersecurity-related awareness and safe behavior online.)
16.	Are all program sites in compliance with the Americans with Disabilities Act?
17.	Has your organization previously received a CISA grant or cooperative agreement? If so, provide year(s)
Program Outcomes (for cooperative agreement-funded services over the one -year period)	
18.	Increased cybersecurity awareness across stakeholder groups.
19.	Enhanced and newly developed materials for cybersecurity awareness.
20.	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, future subrecipient'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.

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

11. 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 perform work under the federal award, a draft [or final signed] Memorandum of Understanding (MOU) between the recipient and the subrecipient must 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 or cooperative agreement programs from which your organization currently

1. 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.

2. Funding Restrictions and Allowable Costs

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

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

3. Allowable Costs

- 1) DHS cooperative agreement funds may only be used for the purpose set forth in the terms of the Federal award, which include the terms of this NOFO, and must be consistent with the statutory authority for the award. Grant or cooperative agreement funds 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) Pre-award costs are allowable only with the written consent of DHS and included in the award agreement.
- 3) **Unallowable Costs.** Cooperative agreement funds may not be used for the following purposes:
 - a. Acquiring or improving real property.
 - b. Foreign Travel.
 - c. Cooperative agreement application development.
 - d. Costs for food or refreshments.
 - e. Incentive items or gift cards.

- f. Cost-sharing or matching funds for other Federal grants or cooperative agreements, lobbying, or intervention in Federal regulatory or adjudicatory proceedings.
- g. Federal funds may not be used to sue the Federal government or any other government entity.

4) Management and Administration (M&A) Costs

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 or subrecipient's personnel are not typically categorized as M&A costs unless the recipient or subrecipient chooses to assign personnel to specific M&A activities

E. Application Review Information

1. Application Evaluation Criteria

a. Programmatic Criteria

The following criteria will be used to evaluate proposals and the total maximum score is 100 points. 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/Cybersecurity Awareness Month (CSAM) activity outcomes/impact by getting stakeholders to absorb messages from these activities and in others carrying Campaign/CSAM 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, DHS 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:

- 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 y

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 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 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 of scores and comments to ensure that every eligible application receives full and fair consideration.
- 3) 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.
- 4) 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, 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.
- 5) 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 Campaign.

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 cooperative agreement award and the terms and conditions associated with responsibilities under 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.

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

2. Unsuccessful Applications

Unsuccessful applicants will be notified by email in a timely manner. There are no appeal rights for unsuccessful applicants that are not selected for a federal award.

3. Administrative and National Policy Requirements

The recipient is required to comply with the DHS Standard Terms and Conditions, which are available online at: DHS Standard Terms and Conditions. In addition, the recipient is 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 renewal 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. 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..

The recipient 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.

4. Reporting

a. Federal Financial Reporting Requirements

The recipient is required to submit the following Federal Financial Reports:

- a. 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. All Reports must be submitted via the Grants Solution System.

- b. 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 must be submitted via the Grants Solution System.

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

- c. Quarterly Federal Financial Reports (Cash Transaction). The Recipient must submit the FFR (SF-425) Federal Cash Transaction Reports to the Department of Health and Human Services, Payment Management System. The Quarterly Cash Transaction reports must 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 Program reports that meet program-specific reporting requirements which 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 must be submitted as a grant note via the Grants Solution System.
- 2) 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 must include cumulative quantitative data, program accomplishments and challenges, and any promising practices related to cybersecurity awareness building. The final report must be submitted as a grant note via the Grants Solution System.

c. Additional Reporting Requirements

Report	Estimated Deadline
Cybersecurity Awareness Campaign 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
Cybersecurity Awareness Month Program Tactical Plan	120 days prior to each CSAM for CSAM commencing after October 2023.
Report of key outcomes from Cybersecurity Awareness Month	30-45 days following conclusion of Cybersecurity Awareness Month
Annual report to CISA of all activities related to the national cybersecurity awareness campaign to include recommendations on next steps.	Annually (based on fiscal year)

1) 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, the recipient must permit DHS, upon reasonable notice, to review cooperative agreement-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 the cooperative agreement program.

2) Closeout Reporting Requirements

Within 120 days after the end of the period of performance, or after an amendment has been issued to close out the cooperative agreement, 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.
- 5) Other documents required by this NOFO, terms and conditions of the award, or other DHS Grants and Financial Assistance Office guidance.

After these reports have been reviewed and approved by DHS Grants and Financial Assistance Office, a closeout notice will be completed to close out the cooperative agreement. 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 the DHS Grants and Financial Assistance Office during the closeout of their prime cooperative agreement 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 grant award with the DHS Grants and Financial Assistance Division, the recipient must notify DHS Grants and Financial Assistance Office 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:

- a) Are presently excluded or disqualified.
- b) 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.
- c) 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).
- d) 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 Office 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, the 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, the 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 the 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 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. pt. 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 cooperative agreement funds, recipients agree to participate in the evaluation, which may include analysis of individuals who benefit from the cooperative agreement, and provide access to program operating personnel and participants, as specified by the evaluator(s) for six months after the period of performance.

5. DHS Awarding Agency Contact Information

a. Contact and Resource Information

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

- 1) 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
Program Officer
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 – CISA – WB2 Stop 0612 -- SED/SRPB AWR
Cybersecurity and Infrastructure Security Agency
4200 Wilson Blvd
Arlington, VA 20598-0645

Current Website Address: <https://www.cisa.gov/cybersecurity-awareness-month>

- 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.

Lisa Johnson
Grants and Financial Assistance Division (GFAD)
Office of Procurement Operations
245 Murray Lane, SW
Mail Stop: 0115, Rm 3051
Washington, D.C. 20528-0115
Phone: (202) 524-8543
Email: Lisa.Johnson1@hq.dhs.gov

6. Other Information

1) Period of Performance Extensions

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

a. 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 must 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 Grants Officer.

2) Prior Approval

The recipient must not, without the prior written approval of DHS, 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 must 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

The recipient must obtain prior approval before earning program income. 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 must be listed in the progress and financial reports.