

**The Department of Homeland Security (DHS)
Notice of Funding Opportunity (NOFO)
National Cyber Security Awareness**

NOTE: If you are going to apply for this funding opportunity and have not obtained a Data Universal Numbering System (DUNS) number and/or are not currently registered in the System for Award Management (SAM), please take immediate action to obtain a DUNS Number, if applicable, and then to register immediately in SAM. It may take 4 weeks or more after you submit your SAM registration before your registration is active in SAM, then an additional 24 hours for Grants.gov to recognize your information. Information on obtaining a DUNS number and registering in SAM is available from Grants.gov at: <http://www.grants.gov/web/grants/register.html> Detailed information regarding DUNS and SAM is also provided in Section D of this NOFO, subsection, Content and Form of Application Submission.

A. Program Description

Issued By

U.S. Department of Homeland Security (DHS), National Protection and Programs Directorate, Office of Cybersecurity and Infrastructure Security Agency (CISA)

Catalog of Federal Domestic Assistance (CFDA) Number

97.128

CFDA Title

National Cyber Security Awareness

Notice of Funding Opportunity Title

National Cyber Security Awareness

NOFO Number

DHS-19-NPPD-128-NCSA-001

Authorizing Authority for Program

Homeland Security Act of 2002 (Public Law 107-296), 6 U.S.C 121

Appropriation Authority for Program

Department of Homeland Security Appropriation Act, 2019 (Public Law 116-6), Title III, Protection, Preparedness, Response, and Recovery, Cybersecurity and Infrastructure Security Agency, Operations and Support.

Program Type

New

Program Overview, Objectives, and Priorities

Program Overview and Priorities

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk manager, empowering partner organizations to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future. As part of this mission, CISA deploys risk management information, tools and technical services to strengthen cybersecurity awareness and practices across government entities, business and the general public.

CISA supports the DHS Cybersecurity mission area and this grant specifically supports DHS Goal 4.2: Promote Cybersecurity Knowledge and Innovation.

Accordingly, CISA requires support in coordinating and collaborating with appropriate private sector and non-profit organizations as well as federal, state, and local government entities to facilitate a comprehensive national cybersecurity awareness campaign. This campaign intends to execute a research-driven strategy focused on implementing specific programs, activities, materials and outreach efforts, building on its established national cybersecurity awareness campaign to include activities and initiatives associated with National Cybersecurity Awareness Month in October.

CISA requires assistance in executing a National campaign that educates at risk segments of the public about the dangers of cyber threats and key actions that can be taken to mitigate risks; identifying effective approaches to increase cybersecurity awareness among the general public and specific target audiences; building relationships and coalitions across cybersecurity stakeholders to support a broad national effort; executing means of measuring impact of campaign strategies on increasing public cybersecurity awareness, and serving 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 the threats and hazards that Americans face.

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

Program Objectives and Activities

The recipient will provide year-long program support and coordination to include researching, planning, executing and measuring project or individual initiative-based activities as part of a holistic strategy to drive cybersecurity actions in the targeted audiences. This is a national-level effort. Viable applicants must ensure

they address capabilities and approach to driving behavior change among national, 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 industry, educational institutions, non-profits and federal, state, local, tribal, and territorial governments as well as international partners. This includes how the recipient will amplify, promote, and bolster DHS's existing cybersecurity awareness work, partnerships, and relationships and enhance these efforts.

Strategy Development

- Assess current and future cybersecurity needs for the general public as well as for targeted segments based on susceptibility 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 program activities to most effectively address cybersecurity risk.
- Develop an annual cybersecurity communications campaign that meets identified needs, addresses the highest risk areas, and is understandable and implementable to the American public, augmented with targeted messaging related to the greatest and most prevalent risks by segmented priority audiences (e.g., home Internet users; small/medium-sized businesses; the academic community including K-12 and higher education educators, administrators, and students).
- Measure, analyze and report on the effectiveness of awareness efforts and associated outcomes, to include:
 - Developing a methodology for measuring successful cybersecurity awareness activity reach and outcomes based on specified performance metrics aligned to overall program objectives.
 - Establishing baselines for awareness and actions associated with cybersecurity practices
 - Conducting research to measure awareness of and outcomes and behavior changes due to Campaign 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

Communications Materials Production

- Create 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 in the development of a coordinated messaging effort with partners in industry, educational institutions, non-profits and federal, state, local, tribal, and territorial governments as well as international partners.
- Engage government stakeholders at the Federal, state, local, tribal and territorial levels in strong coordination with DHS/CISA to enhance the program and promote participation.
- Conduct outreach efforts on cybersecurity awareness through identification of; creation of; and/or engagement in meetings, conferences, events, and initiatives.

Crosspromotion of Cybersecurity Resources

- Promote DHS/CISA cybersecurity programs/resources where applicable and relevant.
- Align awareness/outreach efforts to the CISA strategic plan for long-term success, and regularly refresh and update outreach with new and innovative ideas, content, and strategies to the Campaign.
- Develop and maintain efforts to advance cybersecurity workforce development through cybersecurity awareness communications channels, to include promotion of cybersecurity career opportunities and information across diverse stakeholder groups.

Execute National Cybersecurity Awareness Month Activities

- Design a strategy to engage national participation across partners to raise the visibility of cybersecurity during October, to include tailored activities for small/medium businesses, academia, and the general public.
- Facilitate partnership across cybersecurity stakeholders to execute a comprehensive 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 among the general public and target segments.
- Create, produce and disseminate 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 “kick-off” event.

Program Management

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

Performance Metrics

Through achieving the priorities listed above, DHS/CISA, through the National Cybersecurity Awareness Grant, seeks to:

- Measure short and long-term effects of national understanding of individual roles in cybersecurity.
- Increase in partnerships of cybersecurity messaging campaigns and national cybersecurity awareness month.
- Measures changes in behavior towards enhanced cybersecurity among populations who receive awareness messaging.
- Increase the number of Americans receiving cybersecurity awareness messaging.

B. Federal Award Information

Award Amounts, Important Dates, and Extensions

Available Funding for the NOFO: \$549,996

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

Period of Performance: *12 months*

A second budget period may be funded for an additional 12 months.

Any period over 12 months is an "extension." Extensions to the period of performance are allowable. Please refer to Section H. Additional Information – Extension, for more information regarding what steps recipients must follow and what information must be included in the justification for such request to be considered.

Projected Period of Performance Start Date(s): *06/10/2019*

Projected Period of Performance End Date(s): *06/30/2020*

Funding Instrument Cooperative Agreement

Due to substantial involvement, the best manner in which 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. **Eligibility Information**
Eligible Applicants

Nonprofits with 501(c)(3) IRS status, other than institutions of higher education

Eligible applicants will include public or private non-profit organizations, dedicated to promoting cybersecurity-related awareness and safe behavior online. CISA will not review applications that fail to meet the eligibility criteria.

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 sub-awardee of a non-profit must provide documentation of non-profit and/or public status. This requirement does not apply to for-profit applicants. 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.
 - A signed statement on official letterhead by an official authorized to apply for grant funds on behalf of the public entity shall suffice.

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.

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 document does not include one or more of the required forms or documents listed under Section D. The required forms and documents are:
 - a. Form SF-424 – Application for Federal Assistance
 - b. Form SF-424A – Budget
 - c. Form SF-424B – Assurances – Non-Construction Programs
 - d. Certification Regarding Lobbying
 - e. Budget Narrative and Table
 - f. Project Abstract
 - g. Project Narrative
 - h. Project Plan
 - i. Documentation of non-profit status

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

Cost Share or Match

No cost share is required

D. Application and Submission Information

Key Dates and Times

Date Posted to Grants.gov:	04/08/2019
Application Submission Deadline:	05/09/2019 at 11:59PM [EDT]
Anticipated Funding Selection Date:	05/31/2019
Anticipated Award Date:	06/10/2019

NOTE: The application must be received in Grants.gov by the date and time listed above. If an application is received after the deadline, it will not be considered. Applicant will receive a confirmation from Grants.gov once the application is successfully submitted.

The application is time stamped by the Grants.gov system when submitted and applicants will be notified accordingly. The federal office will download the application if received by the deadline date and time as indicated on the NOFO.

Other Key Dates (*If applicable*).

Event	Suggested Deadline For Completion
Obtaining DUNS 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 to two weeks before actual submission deadline
<i>If applicable additional critical dates</i>	

June 2019: Post Award Conference will be held via teleconference

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 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 write or fax a request to:

Lisa Johnson
Grants Officer
Office of Procurement Operations
245 Murray Lane, SW, Mail Stop 0115
Washington, D.C. 20528-0115
Lisa.Johnson1@hq.dhs.gov
Phone: 202-447-5094

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.

Content and Form of Application Submission

Applicant must submit all required forms and required documents listed in this section. See the Grants.gov [Applicant User Guide](#) for instructions on how to attach forms and documents.

Applicants should ensure the final submitted application package includes all required forms and documents. Applicants should avoid the use of special characters in attachment file names.

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 as long as 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 sub-awardee is proposed under the project, applicants must provide a separate sub-awardee 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 sub-awardee 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						
Category and Item	Year 1			TOTAL		
	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 first and second performance years. Separate the first performance year costs from the second performance year costs. 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.
 - 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 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 sub-awardee FTEs.

16.	Proposed Sub-Awardee Organization (if applicable) (Organization name, point of contact name and title, address, phone number, email address)
17.	Services Proposed by Sub-Awardee 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-awardee'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 sub-awardee organization and how the applicant will manage the sub-awardee. 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 both years of 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 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.

9. Other Attachments

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

- a. Résumés of key personnel (one page each) or job descriptions for key positions if vacant.
- b. If proposing a sub-awardee who will provide additional or complementary grant-funded services, a draft [or final signed] Memorandum of Understanding (MOU) 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.

Unique Entity Identifier and System for Award Management (SAM)

All applicants for this award must:

1. Be registered in SAM before submitting its application;
2. Provide a valid DUNS number in its application; and
3. Continue to maintain an active SAM registration with current information at all times during which it has an active federal award or an application or plan under consideration by a federal awarding agency.

DHS may not make a federal award to an applicant until the applicant has complied with all applicable DUNS and SAM requirements and, if an applicant has not fully complied with the requirements by the time DHS is ready to make a federal 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.

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 applicants to submit their applications online through Grants.gov.

How to Register to Apply through Grants.gov

1. *Instructions:* 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 Data Universal Numbering System (DUNS) 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, refer to: <https://www.grants.gov/web/grants/applicants/registration.html>

Organization applicants can find complete instructions here:

<https://www.grants.gov/web/grants/applicants/organization-registration.html>

2. *Obtain a DUNS Number:* All entities applying for funding, including renewal funding, must have a Data Universal Numbering System (DUNS) number from Dun & Bradstreet (D&B). Applicants must enter the DUNS number in the data entry field labeled "Organizational DUNS" on the SF-424 form.

For more detailed instructions for obtaining a DUNS number, refer to:

<https://www.grants.gov/web/grants/applicants/organization-registration/step-1-obtain-duns-number.html>

3. *Register with SAM:* In addition to having a DUNS number, 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>

4. *Create a Grants.gov Account:* The next step in the registration process is to create an account with Grants.gov. Applicants must know their organization's DUNS number to complete this process.

For more information, follow the on-screen instructions or refer to:

<https://www.grants.gov/web/grants/applicants/registration.html>

5. *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 DUNS Number for the organization in the DUNS 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>

6. *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 Authorized Organization Representative (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>

7. *Track Role Status*: To track your role request, refer to:
<https://www.grants.gov/web/grants/applicants/registration/track-role-status.html>
8. *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 individuals who are able to make legally binding commitments on behalf of the organization as an AOR; **this step is often missed and it is crucial for valid and timely submissions.**

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 Notice of Funding Opportunity, 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>

1. *Create a Workspace*: Creating a workspace allows you to complete it online and route it through your organization for review before submitting.
2. *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.
3. *Adobe Reader*: If you decide not to apply by filling out webforms you can download individual PDF forms in Workspace so that they will appear similar to other Standard or DHS forms. 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>

4. *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.

5. *Complete SF-424 Fields First:* The forms are designed to fill in common required fields across other forms, such as the applicant name, address, and DUNS 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.
6. *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.
7. *Track a Workspace:* After successfully submitting a workspace package, 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 you are applying for.

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.

Timely Receipt Requirements and Proof of Timely Submission

Online Submissions. All applications must be received by **Midnight Eastern Daylight 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. 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.

Intergovernmental Review

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

(See <https://www.archives.gov/federal-register/codification/executive-order/12372.html>; <https://www.whitehouse.gov/wp-content/uploads/2017/11/SPOC-Feb.-2018.pdf>)

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, National Cybersecurity Awareness Month activities and program management.

1. DHS grant or cooperative agreement funds may only be used for the purpose set forth in the Congressional record and must be consistent with the statutory authority for the award. 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. 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. Title of equipment will remain with the Recipient until closeout when disposition will be provided in writing by the DHS within 120 days of submission of final reports.
- e. Equipment purchases are limited to those items that fall within the categories described in Attachment C, "Eligible Equipment."
- f. **Pre-award** costs are allowable only with the written consent of DHS and included in the award agreement.

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

- a. Profit/Fee is not allowable except when subcontracting for routine goods and services with commercial organizations.
- b. Construction costs and purchase of real property.
- c. Foreign Travel.
- d. Funding for direct reimbursement of proposal development.
- e. Costs for food or refreshments.
- f. Incentive Items or gift cards.
- g. General volunteer stipends.
- h. Living allowances for any volunteer service program participants.
- i. 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.
- j. Federal funds may not be used to sue the Federal government or any other government entity.

Management and Administration (M&A) Costs.

Management and Administrative Costs are allowable for the grantee and any proposed sub-awardee (if applicable). For more information on allowable costs, please see Section D, Funding Restrictions and Section D, How to Apply

Indirect Facilities & Administrative (F&A) Costs.

Indirect Costs are allowable for the grantee and any proposed sub-awardee (if applicable). The applicant must attach a copy of the latest indirect cost rate agreement negotiated with a cognizant federal agency. If the applicant is in the process of initially developing or renegotiating a rate, upon notification that an award will be made, it should immediately develop a tentative indirect cost rate proposal based on its most recently completed fiscal year, in accordance with the cognizant agency's guidelines for establishing indirect cost rates, and submit it to the cognizant agency. Applicants awaiting approval of their indirect cost proposals may also request indirect

costs. When an indirect cost rate is requested, those costs included in the indirect cost pool should not also be charged as direct costs to the award. If the applicant is requesting a rate which is less than what is allowed under the program, the authorized representative of the applicant organization must submit a signed acknowledgement that the applicant is accepting a lower rate than allowed.

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

E. Application Review Information

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:

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.

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. NCSD 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 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 sub-awardees and/or its key personnel. This may include publically 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 sub-awardee 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 sufficient 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.

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 is able to 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 is able to 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 with regard to 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 is able to 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 is able to provide methodology for measuring successful Campaign/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 organization 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 state of affairs 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 is able to 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.

Supplemental Financial Integrity Review

If the anticipated federal share of a federal award will be greater than the simplified acquisition threshold, currently \$250,000 (see Section 805 of the National Defense Authorization Act for Fiscal year 2008, Pub. L. No. 115-91, OMB Memorandum M-18-18 at <https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-18.pdf>):

- i. Prior to making a Federal award with a total amount of Federal share greater than the simplified acquisition threshold, DHS is required to review and consider any information about the applicant that is in the designated integrity and performance system accessible through SAM (currently FAPIIS).

- ii. An applicant, at its option, may review information in the designated integrity and performance systems accessible through SAM and comment on any information about itself that a Federal awarding agency previously entered and is currently in the designated integrity and performance system accessible through SAM.
- iii. DHS will consider any comments by the applicant, in addition to the other information in the designated integrity and performance system, in making a judgment about the applicant's integrity, business ethics, and record of performance under Federal awards when completing the review of risk posed by applicants as described in 2 CFR §200.205 Federal awarding agency review of risk posed by applicants."

F. Federal Award Administration Information

Notice of Award

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.

Administrative and National Policy Requirements

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

[DHS Standard Terms and Conditions](#)

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

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 sub-awardees, 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: The Recipient grants the Government a royalty free, non-exclusive and irrevocable license to reproduce, display, distribute copies, perform, disseminate, or prepare derivative works, and to authorize others to do so, for Government 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 sub-awards: The Recipient agrees to include in any sub-award 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

Federal Financial Reporting Requirements.

The Federal Financial Reporting Form (FFR) is available online at:

<https://www.grants.gov/web/grants/forms/post-award-reporting-forms.html>

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 90 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.

Program 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.
2. Final Performance Report must be submitted to the DHS Grants Officer within 90 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.

Additional Information

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 year's NCSAM (year 2)
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	Annually (based on fiscal year)

steps. DHS will review the annual report and determine if there are additional tasks for the grantee.	
---	--

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.

Close Out Reporting Requirements

Within 90 days after the end of the period of performance the recipient must submit a final FFR and final progress report detailing all accomplishments and a qualitative summary of the impact of those accomplishments throughout the period of performance.

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 FAO, a close-out 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 (3) years from the date of the final FFR.

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

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 a federal agency, the recipient must notify the federal agency if it knows of 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. At any time after accepting the award, if the recipient learns that 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 the federal agency in accordance with 2 C.F.R. § 180.350.

G. DHS Awarding Agency Contact Information

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.

Latasha McCord

Cybersecurity Education & Awareness Branch (CE&A)

Phone: 703-705-6672

Email: Latasha.mccord@hq.dhs.gov;

Mailing Address: 245 Murray Ln., SW
Bldg. 410, Stop #640
Washington, D.C. 20528

Current Website Address: <https://www.dhs.gov/stophinkconnect>

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

Grant Officer

Office of Procurement Operations (MGMT OPO)

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

Phone: (202) 447-5904

Email: lisa.johnson1@hq.dhs.gov

H. Additional Information

1. Extensions

Extensions to 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 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.

b. 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.

c. 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.

d. 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.

2. Disclosure

Risk Assessment Evaluation

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

In evaluating risks, DHS may consider the following:

- Financial stability;
- Quality of management systems and ability to meet the management standards prescribed in applicable OMB Guidance;
- Applicant's record in managing previous DHS awards, cooperative agreements, or procurement awards, including:
 1. Timeliness of compliance with applicable reporting requirements
 2. Accuracy of data reported
 3. Conformance to the terms and conditions of previous federal awards
 4. If applicable, the extent to which any previously awarded amounts will be expended prior to future awards
 5. Information available through OMB-designated repositories of government-wide eligibility qualification or financial integrity information, such as: Federal Awardee Performance and Integrity Information System (FAPIIS), Duns and SAM
 6. Reports and findings from single audits performed under Subpart F – Audit Requirements, 2 C.F.R. Part 200 and findings and reports of any other available audits
 7. Applicant organization's annual report
 8. Publicly available information, including information from the applicant organization's website
 9. Applicant's ability to effectively implement statutory, regulatory, or other requirements imposed on award recipients.

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

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.
