



Notice of Funding Opportunity (NOFO)

Global Digital Threat Lab

Bureau for Democracy, Human Rights, and Labor (DRL),

Department of State

Opportunity number: DFOP0019364

Application deadline: August 13, 2026

Contents

A.	Basic Information	3
B.	Eligibility	4
C.	Program Description	5
D.	Application Contents and Format.....	10
E.	Submission Requirements and Deadlines.....	12
F.	Application Review Information.....	17
G.	Award Notices	18
H.	Post-Award Requirements and Administration.....	19
I.	Other Information	22

A. Basic Information

1. Overview

Funding Opportunity Title	Global Digital Threat Lab
Funding Opportunity Number	DFOP0019364
Announcement Type	Initial Announcement
Deadline for Applications	August 13, 2026, 11:59PM EDT
Assistance Listing Number	19.345
Length of performance period	Up to 36 months
Number of awards anticipated	1 award
Award amount	\$2,960,039 (approximately)
Total available funding	\$2,960,039, pending availability of funds
Type of Funding	Fiscal Year 2025, Internet Freedom Earmark, Democracy Funds under the Foreign Assistance Act
Anticipated project start date	September 28, 2026

Funding Instrument Type: Grant or Cooperative Agreement

Project Performance Period: The proposed project should be completed in 36 months or less.

The Department of State will entertain applications for a continuation grant funded under this award beyond the initial budget period on a non-competitive basis subject to availability of funds, satisfactory progress of the program, and a determination that continued funding would be in the best interest of the U.S. Department of State.

This notice is subject to availability of funding.

2. Executive Summary

Freedom of expression online faces threats globally from authoritarian governments employing sophisticated technology to restrict speech, control the flow of information, and chill dissenting voices. These challenges infringe on privacy; access to information; and the exercise of freedoms of expression, peaceful assembly, association, and religion or belief online. The misuse of commercial spyware is increasingly deployed by authoritarian governments and other digital threat actors to suppress dissent and restrict freedom of expression and privacy. Artificial Intelligence (AI) is now facilitating cyberattacks, lowering the barrier of entry for threat actors and improving their efficiency and effectiveness.

Civil society, human rights defenders (HRDs), and other independent voices are frequently targeted by spyware, denial-of-service attacks, phishing, social engineering, and other cyberattacks, yet often are not adequately equipped to deal with a rapidly evolving threat environment. Civil society has limited access to the digital forensics capabilities necessary to identify and remediate digital attacks that leverage advanced technology, such as commercial

spyware. This can lead to malware attacks that go undetected for extended periods of time, allowing attackers to damage systems, collect information, or monitor the activities of their targets. Even when civil society actors succeed in addressing and remediating a particular digital attack, they frequently lack the resources to address the hardware and software vulnerabilities that attackers exploit. These vulnerabilities often result in independent voices being repeatedly targeted and attacked through the same threat vectors. There are existing entities that support civil society in addressing spyware and other advanced digital threats; however, the need for these services is far greater than the current available support.

The U.S. Department of State, Bureau of Democracy, Human Rights, and Labor (DRL) announces an open competition for a global program to protect freedom of expression online by providing digital security support to civil society organizations, human rights defenders (HRDs), and other independent voices. The project will support a new or existing global digital threat lab that will investigate, analyze, report on, prevent, and mitigate the impacts of digital attacks on independent voices. The project will support cybersecurity experts from civil society who understand the digital threats and challenges faced by independent actors working in repressive contexts or on controversial topics that put them at risk of cyberattacks. The program places particular emphasis on addressing advanced digital threats, such as the misuse of commercial spyware and AI-facilitated cyberattacks.

The Department of State is committed to supporting an open, interoperable, secure, and reliable global Internet that enables the exercise of human rights and fundamental freedoms online. This initiative advances the 2025 National Security Strategy by maintaining U.S. leadership in digital innovation, countering digital repression, and defending freedom of expression and access to information. It also supports the Department of State's FY 2026–2030 Agency Strategic Plan by strengthening U.S. technological dominance and using targeted foreign assistance to advance U.S. strategic interests.

B. Eligibility

1. Eligible Applicants

The following organizations are eligible to apply:

- U.S.-based non-profit organizations/nongovernmental organizations (NGOs)
- Foreign-based non-profit organizations/NGOs
- Private or public institutions of higher education
- For-profit organizations or businesses

2. Cost Sharing or Matching

Providing cost sharing, matching, or cost participation is not required for this NOFO and will not improve competitive ranking of an application. Any budget items proposed for cost share must be allowable per 2 CFR 200, Subpart E—Cost Principles.

3. *Other Eligibility Requirements*

All organizations must have a Unique Entity Identifier (UEI) issued via SAM.gov as well as a valid registration in SAM.gov. Please see Section D.3 for more information. Individuals are not required to have a UEI or be registered in SAM.gov.

Primary applicants may submit only one application in response to this NOFO. An applicant may be included as a consortium member and/or subgrantee in other applications from other primary applicants.

C. Program Description

Overview

Authoritarian states and U.S. adversaries frequently use sophisticated technological tools and tactics to target for repression and silence civil society, HRDs, and other independent voices online with surveillance, censorship, and privacy-invasive data collection. Some common approaches include: the misuse of commercial spyware; distributed denial of service (DDoS) attacks; phishing; man-in-the-middle attacks; and social engineering; among many other techniques. Malign actors are also increasingly using AI to increase the efficiency, scale, and effectiveness of cyberattacks.

The misuse of commercial spyware and AI-facilitated cyberattacks by governments to suppress independent voices are of particular concern to the Department. When civil society, HRDs, and other independent actors are targeted through technological tools and tactics, including being surveilled with spyware or other forms of malware, they typically struggle to identify and remediate the issue. Even when they successfully remediate the issue, targeted individuals usually do not have access to the expertise necessary to resolve remaining hardware, software, or social engineering-related vulnerabilities. As a result, victims of cyberattacks increasingly find themselves repeatedly targeted with the same threat vectors. Some existing organizations provide civil society with digital forensics, spyware remediation, and emergency support to mitigate cyberattacks; however, these services are highly technical and in very short supply.

To address these issues, DRL will support an existing or new global lab to (1) track, analyze, and report on digital threat and attack incidents and trends affecting independent voices, and (2) provide digital forensics, incident response, and prevention support and resources to civil society, HRDs, and other independent voices.

U.S. economic and national security interests are inextricably connected to the protection of privacy and the freedoms of expression, peaceful assembly, association and religion or belief online. The Department is therefore committed to researching and addressing online threats to independent voices. Outputs from this program will also provide critical information on the cyberthreat landscape, which supports the U.S. policy priority to protect freedom of expression on the global Internet, and may result in publicly available information be available to support imposing sanctions and visa restrictions against threat actors.

1. Goals and Objectives

Goal: Strengthen freedom of expression online through a new or existing global digital threat lab that supports civil society, HRDs, and other independent voices in identifying, mitigating, and preventing cyberattacks, including commercial spyware attacks.

Objective 1: Increased knowledge and threat information sharing among civil society about technology-based approaches used by governments and other threat actors to target independent voices for repression online.

Project activities will identify, track, and analyze digital attacks and key threats to privacy and the freedoms of expression, peaceful assembly, association and freedom of religion or belief online, with a particular focus on commercial spyware and other advanced digital attack methods. The project will produce applied research products that are designed to inform civil society, HRDs, and other independent voices about digital threats globally, as well as new developments in digital repression tactics. Topics may include, but are not limited to, evolving trends in the misuse of commercial spyware and other advanced repressive tools used against civil society; analysis of recent cyberattacks against independent voices; the impact of AI on digital repression tactics; and broader trends in the digital security space. Research should equip independent groups worldwide with relevant and actionable cybersecurity information.

Activities will include reporting and disseminating digital threat information and research findings on a global scale to independent actors at high risk of spyware and other cyberattacks. The project should develop a variety of accessible products in formats and media appropriate to at-risk groups to improve their ability to identify, prevent, and mitigate digital attacks and threats. Examples of research products include, but are not limited to, case studies, website articles, briefers, research reports, and white papers. Ideally, research should include threat tracking that provides continuously updated information, such as through interactive tracking tools. Applicants are encouraged to propose innovative means of reaching their target audiences that are tailored to the independent groups they seek to inform. Research products must be provided to DRL and must be made freely and publicly available unless compelling security, legal, privacy, ethical, and/or technical justifications exist. Examples of reasonable exceptions include situations in which a digital attack has not been fully remediated, an exploited vulnerability has not been addressed, or disclosing information poses a clear risk to groups the project supports. DRL must approve any restrictions on the availability and accessibility of research products.

Applicants must clearly articulate how activities will complement or add to existing research, tracking, and/or mapping initiatives, rather than duplicating them. Proposed research must demonstrate a strong baseline understanding of the issue areas, as well as a clear and direct connection between research topics and the protection of privacy and/or the freedoms of expression, peaceful assembly, association and religion or belief online. Competitive applications will also demonstrate a plan for ensuring sustainability of the project's research activities.

Objective 2: Improved prevention, mitigation, and access to remedy for independent voices targeted by spyware and other advanced cyberattacks online.

The global digital threat lab will support civil society, HRDs, and other independent voices in identifying cybersecurity threats, addressing emergency cybersecurity incidents, securing digital systems impacted by attacks, implementing preventive measures, and conducting advanced digital forensics. Activities will counter cyberattacks aimed at restricting freedom of expression online, with a focus on advanced attack methodologies, such as the misuse of commercial spyware.

Illustrative activities under Objective 2 could include but are not limited to:

- Conduct advanced digital forensics to identify digital attack mechanisms, recommend and/or perform remediation actions, and share threat information.
- Support existing help desks (or create new ones if context and circumstances warrant) to address emergency digital security incidents.
- Strengthen peer-to-peer networks of civil society, HRDs, and other independent voices to share information, tactics, and experiences that improve their digital security posture, particularly with regard to spyware and other advanced cyberattacks.
- Develop subject matter experts and/or trainers from target groups that serve as peer-to-peer digital security resources for civil society, HRDs, and other independent voices, particularly with regard to spyware and other advanced cyberattacks.
- Collaborate with existing digital security resource centers and/or threat labs (or create new ones if warranted) to improve threat information sharing, advance best practices, and/or create other force-multiplying impacts.
- Develop or update guidebooks or other technical resources to address evolving threats related to spyware and other acute cybersecurity attacks.
- Conduct digital security audits and develop digital security improvement plans to address vulnerabilities to digital attacks.
- Develop and provide customized training, workshops, and/or ongoing technical support on specific attack and threat trends.

Project activities may cover a range of topics that address the needs of particular independent voices targeted for repression by authoritarian governments and other digital threat actors online. Depending on needs, topics could include: commercial spyware; advanced cybersecurity hygiene for individuals and organizations; phishing, malware, and other forms of cyberattacks; encryption and privacy; and/or the impact of AI on digital repression tactics. Focus topics must not be duplicative of information already widely available for civil society actors, and should instead focus on generating new knowledge about evolving digital threats and how to prevent or remediate them.

Activities should have a clear focus on (1) protecting online privacy and/or the freedoms of expression, peaceful assembly, association and religion or belief, and (2) threats from commercial spyware and other cyberattacks targeting independent voices. Applicants should demonstrate a strong understanding of adversarial efforts, along with a strategy for addressing them that clearly describes any security improvement methods that will be deployed. Any educational resources produced or updated under the project should not be restricted to program

participants, and should be made widely available to other digital security providers and independent groups targeted for repression, unless compelling justifications exist. DRL must approve any restrictions on the availability and accessibility of educational products. Applications should include a plan for ensuring sustainability of the digital security resources created under the project.

Programs may provide targeted independent groups with software licenses or other products on a limited basis to reduce the risk or impact of a specific recent digital attack or a specific near-term threat they are likely to face. Applicants should avoid proposing purchases of hardware or licenses for technology products or services that cannot be used safely and responsibly in relevant repressive, fragile, and/or conflict-affected environments.

Applications must not conduct digital literacy training without a clearly articulated impact for specific at-risk beneficiaries and must not focus on countering remote offline surveillance. Activities must not focus on moderating or otherwise restricting online content unless the applicant explicitly and strictly restricts efforts to methods that do not curtail privacy and the freedoms of expression, peaceful assembly, association and religion or belief.

Projects must have a clear plan to ensure that research and analysis conducted under Objective 1 informs and is integrated into activities under Objective 2. Similarly, applications must demonstrate a clear plan to apply lessons learned from Objective 2 implementation to inform and update research and reporting activities in Objective 1 on an ongoing basis. The two objectives are designed to be integrated and complementary.

Anticipated Results

DRL anticipates that the program will result in the establishment or expansion of a global digital threat lab that fosters:

- Improved identification and understanding of global digital threats that suppress the exercise of freedom of expression online, particularly the misuse of commercial spyware and other cyberattacks targeting civil society, HRDs and other independent voices.
- Increased ability of independent voices globally to prevent and mitigate digital threats, particularly the misuse of commercial spyware and other cyberattacks.

The project's monitoring and evaluation plan should include a limited number of DRL Internet freedom standardized indicators that effectively track the results above. Customized indicators are also permitted on a limited basis. This plan should be comprised of a mix of output and outcome indicators with clear targets for each project year and the life of the project. Applicants are encouraged to consider qualitative data collection in addition to quantitative data to fully assess the impact of the project on the freedom of expression of independent voices online.

Technical Areas of Interest

The following digital threats are particular priorities for the Department under this project:

- The misuse of commercial spyware to surveil civil society, HRDs and other independent voices, contributing to the censorship and repression of independent voices online.

- Other types of cyberattacks specifically targeted at restricting privacy and the freedoms of expression, peaceful assembly, association and religion or belief online. These may include but are not limited to malware deployment, phishing, and access restrictions such as Denial of Service and DDoS attacks.
- The use of AI to facilitate, scale, and/or improve the efficiency of cyberattacks directed at repressing independent voices online.

Geographic Focus

This program seeks to increase knowledge and improve information sharing, skills, and services related to digital attacks affecting independent voices globally. Applicants should propose to identify, research, and mitigate threats that have broad global relevance, and should suggest approaches capable of supporting a wide range of independent civil society and HRD voices from repressive contexts throughout the world. Activities should be relevant and applicable to at least three State Department-defined regions, listed here in order of priority for this program: East Asia and the Pacific, Europe and Eurasia, the Western Hemisphere, North Africa and the Middle East, South and Central Asia, and (Sub-Saharan) Africa.

Risk Management

Competitive applications for this project will also exhibit a clear understanding of the operational risks affecting independent voices in repressive contexts. Applications should include a risk management plan specific to the target groups. Applicants should show consideration for how work under the program might positively and negatively interact with high-risk local contexts to impact the safety and security of the independent voices the project supports. Applicants should not suggest activities that cannot be implemented with the target groups in a relatively safe and responsible manner. For any proposed in-person or virtual activities related to specific highly repressive environments, applications should outline risk mitigation considerations and procedures. Competitive applicants and proposed subgrantees will have deep expertise in risk management and operational security, with a history of successful implementation of similar programs in high-risk environments.

Organizational Structure

Applications should clearly articulate how the global digital threat lab will function as a distinct entity. The program may (1) establish the lab as a new independent entity, (2) set up the lab as a new branch, division, center, or other similar sub-unit within an existing entity, or (3) support an existing lab that already functions as an independent entity or a branch, division, center, or other similar sub-unit within an existing entity. Activities under the program should all be conducted under the auspices of a specifically identified entity or a branch, division, center, or other type of sub-unit within a larger entity. Applications must demonstrate knowledge of existing organizations and entities that provide similar threat analysis and remediation services to civil society, and propose activities that are complementary to existing efforts.

Applicants must also demonstrate collaboration with other organizations and experts to leverage a variety of knowledge, skills, and abilities to successfully implement the activity. DRL

encourages applicants to consider a consortium-based implementing model, given that the program has a global scope and requires diverse capabilities, including research, threat information sharing, digital attack mitigation, and digital forensics. Applications must involve substantial and substantive subgrant, contracting, and/or partnership arrangements with multiple organizations and experts to ensure activities are feasible, technically sound, and appropriate for the target groups. DRL recommends a minimum of thirty percent of funding be dedicated to subgrants and subcontracts to work with small implementing partners, unless there are clearly demonstrated and articulated limitations in the application documents. Applicants should demonstrate their understanding of the program requirements through both the structure of their partnerships and a demonstrated capability to establish and manage such arrangements.

2. Substantial Involvement

If a cooperative agreement is determined to be the most appropriate implementing mechanism, the Department of State will be substantially involved in carrying out the following various aspects of this cooperative agreement. Examples of substantial involvement may include but are not limited to:

- **Workplan:** DRL will play an active role in shaping overall program strategy and will approve the project workplan.
- **Key Personnel:** DRL will approve key personnel. On this project, key personnel will include a Project Director. Additional key personnel roles may be proposed by the applicant and/or DRL prior to award.
- **Subaward and Subcontract selection:** DRL will review and approve all subaward and subcontract agreements before they are finalized.
- **Program Coordination:** DRL will help coordinate and deconflict with other related donor-funded initiatives, using its unique convening power to ensure cross fertilization when beneficial.
- **Ongoing policy and technical consultations:** DRL will participate in regular monthly check-ins (unless otherwise determined by the GOR) and technical review discussions with the project implementers.

The specific review and approval points and procedures for DRL's substantial involvement will be negotiated with the successful applicant prior to award issuance and reflected in the final award.

D. Application Contents and Format

Please follow all instructions below carefully. Proposals that do not meet the requirements of this announcement or fail to comply with the stated requirements will be ineligible.

Content of Application

Please ensure:

- The proposal clearly addresses the goals and objectives of this funding opportunity

- All documents are in English
- All budgets are in U.S. dollars
- All pages are numbered
- All documents are formatted to fit 8 ½ x 11 paper, and
- All Microsoft Word documents are single-spaced, 12 point Times New Roman font, with a minimum of 1-inch margins. Captions and footnotes may be in 10-point font. Font sizes in charts and tables, including the budget, can be reformatted to fit within one page width.

The following documents are **required**:

1. Mandatory application forms

- SF-424 (Application for Federal Assistance – organizations) or SF-424-I (Application for Federal Assistance --individuals)
- SF-424A (Budget Information for Non-Construction programs)
- SF-424B (Assurances for Non-Construction programs)

2. Summary Page (optional)

Cover sheet stating the applicant's name and organization, proposal date, program title, program period proposed start and end date, and brief purpose of the program.

3. Proposal (15 pages maximum)

The proposal should contain sufficient information that anyone not familiar with it would understand exactly what the applicant wants to do. You may use your own proposal format, but it must include all the items below.

- **Proposal Summary:** Short narrative that outlines the proposed project, including project objectives and anticipated impact.
- **Introduction to the Organization or Individual applying:** A description of past and present operations, showing ability to carry out the program, including information on all previous grants from the State Department and/or U.S. government agencies.
- **Problem Statement:** Clear, concise and well-supported statement of the problem to be addressed and why the proposed program is needed
- **Project Goals and Objectives:** The “goals” describe what the program is intended to achieve. The “objectives” refer to the intermediate accomplishments on the way to the goals. These should be achievable and measurable.
- **Project Activities:** Describe the program activities and how they will help achieve the objectives.
- **Project Methods and Design:** A description of how the program is expected to work to solve the stated problem and achieve the goal. Include a logic model as appropriate.
- **Proposed Project Schedule and Timeline:** The proposed timeline for the program activities. Include the dates, times, and locations of planned activities and events.
- **Key Personnel:** Resumes are not required at this time. Instead, provide only the selection criteria your program will apply throughout the grant period of performance when filling key positions.

- **Project Partners:** List the names and type of involvement of key partner organizations and sub-awardees.
- **Project Monitoring and Evaluation Plan:** This is an important part of successful grants. Throughout the timeframe of the grant, how will the activities be monitored to ensure they are happening in a timely manner, and how will the program be evaluated to make sure it is meeting the goals of the grant?
- **Future Funding or Sustainability** Applicant's plan for continuing the program beyond the grant period, or the availability of other resources, if applicable.

4. Budget Justification Narrative

After filling out the SF-424A Budget (above), use a separate file to describe each of the budget expenses in detail. See section *I. Other Information: Guidelines for Budget Submissions* below for further information.

5. Attachments

- Key personnel position descriptions. Resumes are not required at this time. Instead, provide only the selection criteria your program will apply throughout the grant period of performance when filling key positions.
- Letters of support from program partners describing the roles and responsibilities of each partner
- If your organization has a Negotiated Indirect Cost Rate Agreement (NICRA) and includes NICRA charges in the budget, include your latest NICRA as a PDF file.
- Official permission letters, if required for program activities

E. Submission Requirements and Deadlines

1. Address to Request Application Package

Application forms required above are available at <https://www.grants.gov/forms/>.

2. Department of State Contacts

If you have any questions about the grant application process, please contact: DRL-PRU-Solicitation@state.gov.

Questions and Answers or FAQ will be posted on www.grants.gov to answer questions from all potential applicants.

For assistance with MyGrants accounts and technical issues related to the system, please contact the ILMS help desk by phone at +1 (888) 313-4567 (toll charges apply for international callers) or through the Self Service online portal that can be accessed from <https://afsitsm.servicenowservices.com/ilms>. Customer support is available 24/7.

For assistance with Grants.gov accounts and technical issues related to using the system, please call the Contact Center at +1 (800) 518-4726 or email support@grants.gov. The Contact Center is available 24 hours a day, seven days a week, except federal holidays.

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

Required Registrations

All organizations, whether based in the United States or in another country, must have a Unique Entity Identifier (UEI) and an active registration in SAM.gov. A UEI is one of the data elements mandated by Public Law 109-282, the Federal Funding Accountability and Transparency Act (FFATA), for all Federal awards. An applicant must maintain an active registration while it has a proposal under review by the Department and must continue to keep the registration active for the entire duration of the period of performance of any Federal award that results from this NOFO.

The 2 CFR 200 requires subrecipients to obtain a UEI. Please note the UEI for subrecipients is not required at the time of application but will be required before an award is processed and/or directed to a subrecipient.

Note: The process of obtaining or renewing a SAM.gov registration may take anywhere from 4-8 weeks. Please begin your registration as early as possible.

- Organizations **based in the United States** or that pay employees within the United States will need an Employer Identification Number (EIN) from the Internal Revenue Service (IRS) and a UEI prior to registering in SAM.gov.
- Organizations **based outside of the United States** and that do not pay employees within the United States do not need an EIN from the IRS but do need a UEI prior to registering in SAM.gov.
- **Organizations based outside of the United States that do not intend to apply for U.S. Department of Defense (DoD) awards are no longer required to have a NATO Commercial and Government Entity (NCAGE) code to apply for non-DoD foreign assistance funding opportunities.** If an applicant organization is mid-registration and wishes to remove an NCAGE code from their SAM.gov registration, the applicant should submit a help desk ticket (“incident”) with the Federal Service Desk (FSD) online at www.fsd.gov using the following language: “I do not intend to seek financial assistance from the Department of Defense. I do not wish to obtain an NCAGE code. I understand that I will need to submit my registration after this incident is resolved in order to have my registration activated.”

Organizations based outside of the United States and that DO NOT plan to do business with the DoD should follow the below instructions:

Step 1: Proceed to SAM.gov to obtain a UEI and complete the SAM.gov registration process. SAM.gov registration must be renewed annually.

Organizations based outside of the United States and that DO plan to do business with the DoD in addition to Department of State should follow the below instructions:

Step 1: Apply for an NCAGE code by following the instructions on the NSPA NATO website linked below:

NCAGE Homepage:

<https://eportal.nspa.nato.int/AC135Public/sc/CageList.aspx>

NCAGE Code Request Tool (NCRT):

[NCAGE Code Request Tool \(nato.int\)](#)

Exemptions

An exemption from the UEI and sam.gov registration requirements may be permitted on a case-by-case basis. See [2 CFR 25.110](#) for a full list of exemptions.

Organizations requesting exemption from UEI or SAM.gov requirements must email the point of contact listed in the NOFO at least two weeks prior to the deadline in the NOFO providing a justification of their request. Approval for a SAM.gov exemption must come from the warranted Grants Officer before the application can be deemed eligible for review.

4. Submission Dates and Times

Applications are due no later than August 13th, 2026, 11:59PM, EDT

5. Funding Restrictions

i. Funding Restrictions for the United Nations Relief and Works Agency (UNRWA)

None of the funds awarded resulting from this Notice of Funding Opportunity may be made available for subawards, direct financial support, or otherwise used to provide any payment or transfer to United Nations Relief and Works Agency (UNRWA).

ii. Prohibition on Funding Activities that Encourage Mass-Migration Caravans towards the United States Southwest Border

None of the funds awarded under this grant may be made available to encourage, mobilize, publicize, or manage mass-migration caravans towards the United States southwest border. Funds may not be made available for legal counseling on the United States asylum process; and/or for referrals to legal representation in the United States.

Funds may only be used for cash cards for use in the country in which they are provided or to facilitate assisted voluntary returns and other purposes that do not encourage, mobilize, publicize, or manage mass migration caravans towards the United States southwest border. The provision of humanitarian assistance is permitted.

iii. Certification Regarding Compliance with applicable Federal anti-discrimination laws

If the place of performance or delivery of any award made under this NOFO will be within the United States, applicants are advised that they will be required to certify the following at the time of award:

- 1) Its compliance in all respects with all applicable Federal anti-discrimination laws is material to the government's payment decisions for purposes of section 3729(b)(4) of title 31, United States Code and;
- 2) It does not operate any programs promoting Diversity, Equity, and Inclusion that violate any applicable Federal anti-discrimination laws. A program promoting Diversity, Equity, and Inclusion means a program whose purpose is to promote preferences based on race, color religion, sex, or national origins, such as in training or hiring.

iv. Certification Regarding Compliance with 20 U.S.C. 1011f and any other applicable foreign funding disclosure requirements

Applicants are advised that International Higher Education institutes (IHEs) must certify the following at the time of award, and that this certification requirement must be included in any subaward agreements to IHEs:

- 1) Its compliance in all respects with section 1011f of title 20, United States Code, and any other applicable foreign funding disclosure requirements is material for purposes of section 3729 of title 31, United States Code, and for receipt of appropriate Federal grant funds.

v. Certification of Trafficking in Persons Compliance and Compliance Plan

Applicants are advised that they will be required to certify the following at the time of award for awards where the estimated value of services to be performed outside the United States exceeds \$500,000:

-

- 1) To the best of the Recipient's knowledge, neither the Recipient, nor any subrecipient, contractor, or subcontractor of the Recipient or any agent of the recipient or of such a subrecipient, contractor, or subcontractor, is engaged in any of the activities described in [2 CFR 175.105\(a\)](#);

The recipient has implemented a Trafficking in Persons compliance plan to prevent activities described in [2 CFR 175\(a\)](#) and is compliant with this plan; and the compliance plan must follow the minimum requirements

described in 2 CFR 175(b)(5).

- 2) That the Recipient has and will implement procedures to prevent activities described in [2 CFR 175.105\(a\)](#) and to monitor, detect, and terminate any subrecipient, contractor, subcontractor, or employee of the recipient engaging in these activities.

Recipients do not need to submit a copy of the plan. However, they must provide it to the Grants Officer upon request, and as appropriate, must post the useful and relevant contents of the plan or related materials on their website and at the workplace. Recipients must re-certify on an annual basis for the entire award period of performance.

- vi. Prohibition on Unmanned Aircraft Systems (UAS). If your project involves the purchase or use of an UAS, see this [link](#) for requirements and information you must include in your application.
- vii. Promoting Human Flourishing in Foreign Assistance (PHFFA)

Applicants for foreign assistance awards should be aware of requirements in 2 CFR Part 602, 603, and 604.

These policies are referred to collectively as the Promoting Human Flourishing in Foreign Assistance (PHFFA) Policy.

[602](#): The award term imposes certain abortion-related requirements on foreign nongovernmental organizations (NGOs), United States NGOs, public international organizations, foreign governments, and parastatals.

[603](#): The award term imposes certain requirements relating to gender ideology on foreign nongovernmental organizations (NGOs), United States NGOs, international organizations, foreign governments, and parastatals.

[604](#): The award term imposes certain requirements relating to discriminatory equity ideology on foreign nongovernmental organizations (NGOs), United States NGOs, international organizations, foreign governments, and parastatals.

The Department recognizes there are costs associated with these policies. Potential one-time and recurring costs the Department identifies for recipients and grantees are for familiarization with the policy, development and delivery of organizational training and implementation guidance, routine compliance monitoring, and recordkeeping and reporting requirements.

6. Other Submission Requirements

All application materials must be submitted electronically through www.Grants.gov or MyGrants. DRL is not responsible for disqualification due to applicants not being registered before the due date, system or technical errors in MyGrants or Grants.gov, or other errors in the application process.

Applicants must save a screenshot of the checklist showing all documents submitted in case any document fails to upload successfully.

DRL encourages organizations to **submit applications during normal business hours** (Monday – Friday, 9:00 AM-5:00 PM ET). If an applicant experiences technical difficulties and has contacted the appropriate help desk but is not receiving timely assistance (e.g., no response within 48 hours), they may contact the DRL point of contact listed in the NOFO in Section E.2. The point of contact may assist in contacting the appropriate help desk.

F. Application Review Information

1. Review Criteria

Each application will be evaluated and rated based on the evaluation criteria outlined below.

Quality and Feasibility of the Program Idea: The program idea is well developed, with detail about how program activities will be carried out. The proposal includes a reasonable implementation timeline. The proposal does not include any activities contrary to any standing Executive Orders. For a full list, see <https://www.federalregister.gov/>.

Organizational Capacity and Record on Previous Grants: The organization has expertise in its stated field and has the internal controls in place to manage federal funds. This includes a financial management system and a bank account. If sub-awards are proposed, applicant demonstrates experience managing subawards.

Program Planning/Ability to Achieve Objectives: Goals and objectives are clearly stated, and program approach is likely to provide maximum impact in achieving the proposed results.

Budget: The budget justification is detailed. Costs are reasonable in relation to the proposed activities and anticipated results. The budget is realistic, accounting for all necessary expenses to achieve proposed activities.

Monitoring and Evaluation Plan: Applicant demonstrates it is able to measure program success against key indicators and provides milestones to indicate progress toward goals outlined in the proposal. The program includes output and outcome indicators and shows how and when those will be measured.

Sustainability: Program activities will continue to have positive impact after the end of the program.

2. *Indirect Costs*

If two or more applications receive equivalent scores based on the evaluation criteria outlined in this NOFO, preference will be given to the applicant with the lower indirect cost rate, as consistent with Executive Order 14332, Section 4(b)(iii). This preference will only be applied as a tie-breaking mechanism and does not supersede the primary evaluation criteria.

3. *Review and Selection Process*

A review committee will evaluate all eligible applications.

4. *Risk Review*

i. Risk factors

Under the merit review as required by 2 CFR 200.206, prior to making a Federal Award the Department will review and consider the following risk factors:

- a. Financial stability
- b. Management systems and standards
- c. History of performance
- d. Audit reports and findings
- e. Ability to effectively implement requirements

ii. Responsibility/Qualification Information in SAM.gov

The Federal awarding agency, prior to making a Federal award with a total amount of Federal share greater than the simplified acquisition threshold, is required to review and consider any information about the applicant that is in the U.S. government designated integrity and performance system accessible through SAM.gov (see 41 U.S.C. 2313)

An applicant can review and comment on any information in the responsibility/qualification records available in SAM.gov.

Before making decisions in the risk review required by 2 CFR 200.206, the Department will consider any comments by the applicant, along with information available in the responsibility/qualification records in SAM.gov.

G. Award Notices

The award or cooperative agreement will be written, signed, awarded, and administered by the Grants Officer. The award agreement is the authorizing document, and it will be provided to the

recipient for review and counter-signature. The recipient may only start incurring project expenses beginning on the start date shown on the award document signed by the Grants Officer.

If a proposal is selected for funding, the Department of State has no obligation to provide any additional future funding. Renewal of an award to increase funding or extend the period of performance is at the discretion of the Department of State.

Issuance of this NOFO does not constitute an award commitment on the part of the U.S. government, nor does it commit the U.S. government to pay for costs incurred in the preparation and submission of proposals. Further, the U.S. government reserves the right to reject any or all proposals received.

Payment Method:

Payments under this award will be made through the U.S. Department of Health and Human Services (HHS) Payment Management System (PMS).

Recipients may not draw down funds without the affirmative authorization of the Department of State. In addition, recipients must submit, with each PMS payment request, a detailed explanation justifying the request.

H. Post-Award Requirements and Administration

1. Administrative and National Policy Requirements

Before submitting an application, applicants should review all the terms and conditions and required certifications which will apply to this award, to ensure that they will be able to comply. These include:

In accordance with the Office of Management and Budget's guidance located at 2 CFR part 200, all applicable Federal laws, and relevant Executive guidance, the Department of State will review and consider applications for funding, as applicable to specific programs, pursuant to this notice of funding opportunity in accordance with the following:

- [Guidance for Grants and Agreements in Title 2 of the Code of Federal Regulations](#) (2 CFR), as updated in the Federal Register's 89 FR 30046 on April 22, 2024, particularly on:
 - Selecting recipients most likely to be successful in delivering results based on the program objectives through an impartial process of evaluating Federal award applications (2 CFR part 200.205),
 - Promoting the freedom of speech and religious liberty in alignment with *Promoting Free Speech and Religious Liberty* (E.O. 13798) and *Improving Free Inquiry, Transparency, and Accountability at Colleges and Universities* (E.O. 13864) (§§ 200.300, 200.303, 200.339, and 200.341),
 - Providing a preference, to the extent permitted by law, to maximize use of goods, products, and materials produced in the United States (2 CFR part 200.322), and

- Terminating agreements pursuant to the U.S. Department of State Standard Terms and Conditions, including, to the greatest extent authorized by law, if an award no longer effectuates the program goals or agency priorities (2 CFR part 200.340). For the avoidance of doubt, the Department has sole discretion over the determination that an award no longer effectuates program goals or agency priorities, and this provision permits awards to be terminated at the Department's convenience, including when it determines that the award no longer advances the national interest.
- [2 CFR 25 - UNIVERSAL IDENTIFIER AND SYSTEM FOR AWARD MANAGEMENT](#)
- [2 CFR 170 - REPORTING SUBAWARD AND EXECUTIVE COMPENSATION INFORMATION](#)
- [2 CFR 175 - AWARD TERM FOR TRAFFICKING IN PERSONS](#)
- [2 CFR 182 - GOVERNMENTWIDE REQUIREMENTS FOR DRUG-FREE WORKPLACE \(FINANCIAL ASSISTANCE\)](#)
- [2 CFR 183 - NEVER CONTRACT WITH THE ENEMY](#)
- [2 CFR 600 – DEPARTMENT OF STATE REQUIREMENTS](#)
- [U.S. DEPARTMENT OF STATE STANDARD TERMS AND CONDITIONS](#)
- Recipients must comply with all applicable Executive Orders. A searchable list can be found in the Federal Register: <https://www.federalregister.gov/>

2. *Reporting*

Reporting Requirements: Recipients will be required to submit financial reports and program reports. The award document will specify what reports are required and how often these reports must be submitted.

The Federal Financial Report (FFR or SF-425) is the required form for financial reports and must be submitted in PMS, and a copy of the report submitted in PMS then uploaded to the award file in MyGrants. Program reports uploaded to the award file in MyGrants must include a narrative as described below, as well as Program Indicators (or other mutually agreed upon format approved by the Grants Officer). Indicators will be reviewed and negotiated during the final stages of issuing an award on a program-by-program basis.

Narrative progress reports should reflect the focus on measuring the program's progress on the overarching objectives and should be compiled according to the objectives, outcomes, and outputs as outlined in the award's Scope of Work (SOW) and in the Monitoring, Evaluation, and Learning Narrative. An assessment of the overall project's achievements

should be included in each progress report. Where relevant, progress reports should include the following sections:

- Relevant contextual information (limited)
- Explanation and evaluation of significant activities of the reporting period and how the activities reflect progress toward achieving objectives, including meeting benchmarks/targets as set in the approved Monitoring, Evaluation, and Learning Plan. In addition, attach the Monitoring, Evaluation, and Learning Plan, comparing the target and actual numbers for the indicators
- How relevant communities are being included in program activities
- Any qualitative impact or success stories from the project, when possible
- Copy of baseline, mid-term, and/or final evaluation report(s) conducted by an external evaluator; if applicable
- Relevant supporting documentation or products related to the project activities (such as articles, meeting agendas, participant surveys, photos, manuals, etc) as separate attachments
- Any problems/challenges in implementing the project and a corrective action plan with an updated timeline of activities
- Reasons why established goals were not met
- Data for the required indicator(s) for the quarter as well as aggregate data by fiscal year
- Program Indicators or other mutually agreed upon format approved by the Grants Officer
- Proposed activities for the next quarter
- Additional pertinent information, including analysis and explanation of cost overruns or high unit costs, if applicable

A final narrative and financial report must also be submitted within 120 days after the expiration of the award.

Foreign Assistance Data Review: As required by Congress, the Department of State must make progress in its efforts to improve tracking and reporting of foreign assistance data through the Foreign Assistance Data Review (FADR). The FADR requires tracking of foreign assistance activity data from budgeting, planning, and allocation through obligation and disbursement. Successful applicants will be required to report and draw down federal funding based on the appropriate FADR Data Elements, indicated within their award documentation. In cases of more than one FADR Data Element, typically program or sector and/or regions or country, the successful applicant will be required to maintain separate accounting records.

Applicants should be aware of the post award reporting requirements reflected in [2 CFR 200 Appendix XII—Award Term and Condition for Recipient Integrity and Performance Matters](#).

3. **Branding and Marking**

The Department of State, its programs, and U.S. Government funding and assistance should be easily identifiable to the Department's global audiences.

Recipients of federal assistance awards must follow the branding guidance published at [Guidance for Contracts and Grants - U.S. Department of State Brand System](#). Branding policy exceptions are outlined in the U.S. Department of State Foreign Affairs Manual [10 FAM 416, Policy Exceptions](#).

For more information, visit: <https://brand.america.gov/>

I. Other Information

Guidelines for Budget Justification

Personnel and Fringe Benefits: Describe the wages, salaries, and benefits of temporary or permanent staff who will be working directly for the applicant on the program, and the percentage of their time that will be spent on the program.

Travel: Estimate the costs of travel and per diem for this program, for program staff, consultants or speakers, and participants/beneficiaries. If the program involves international travel, include a brief statement of justification for that travel.

Equipment: Describe any machinery, furniture, or other personal property that is required for the program, which has a useful life of more than one year (or a life longer than the duration of the program), and costs at least \$10,000 per unit.

Supplies: List and describe all the items and materials, including any computer devices, that are needed for the program. If an item costs more than \$10,000 per unit, then put it in the budget under Equipment.

Contractual: Describe goods and services that the applicant plans to acquire through a contract with a vendor. Also describe any sub-awards to non-profit partners that will help carry out the program activities.

Other Direct Costs: Describe other costs directly associated with the program, which do not fit in the other categories. For example, shipping costs for materials and equipment or applicable taxes. All “Other” or “Miscellaneous” expenses must be itemized and explained.

Indirect Costs: These are costs that cannot be linked directly to the program activities, such as overhead costs needed to help keep the organization operating. If your organization has a Negotiated Indirect Cost Rate (NICRA) and includes NICRA charges in the budget, attach a copy of your latest NICRA. Organizations that have never had a NICRA may request indirect costs of 15% of Modified Total Direct Costs as defined in 2 CFR 200.1.

“Cost Sharing” refers to contributions from the organization or other entities other than the U.S. Embassy. It also includes in-kind contributions such as volunteers’ time and donated venues.

Alcoholic Beverages: Please note that award funds cannot be used for alcoholic beverages.