Department of State
Public Notice

Bureau of Democracy, Human Rights, and Labor Request for Statements of Interest: DRL FY22 Internet Freedom Annual Program Statement Round 2

I. Requested Objectives for Statements of Interest

Within each of the below Internet Freedom funding themes, DRL The Bureau of Democracy, Human Rights, and Labor (DRL) announces a Request for Statements of Interest (RSOI) from organizations interested in submitting Statements of Interest (SOI) for programs that support Internet Freedom. DRL's goal is to protect the open, interoperable, secure, and reliable Internet by promoting fundamental freedoms, human rights, and the free flow of information online through integrated support to civil society for technology, digital safety, policy and advocacy, and applied research programs. DRL invites organizations interested in potential funding to submit SOI applications outlining program concepts that reflect this goal.

PLEASE NOTE: DRL strongly encourages applicants to immediately access SAMS Domestic or www.grants.gov in order to obtain a username and password. For instructions on how to register with SAMS Domestic for the first time, please refer to the Proposal Submission Instructions for Statements of Interest at: https://www.state.gov/bureau-of-democracy-human-rights-and-labor/programs-and-grants/.

The submission of a SOI is the first step in a two-part process. Applicants must first submit a SOI, which is a concise, 3-page concept note designed to clearly communicate a program idea and its objectives before the development of a full proposal application. The purpose of the SOI process is to allow applicants the opportunity to submit program ideas for DRL to evaluate prior to requiring the development of full proposal applications. Upon review of eligible SOIs, DRL will invite selected applicants to expand their ideas into full proposal applications.

SOIs that move forward to be funded based on this Notice should expect program activities to begin no earlier than August or September of 2023 pending the availability of funds. This is the last *DRL Internet Freedom Annual Program Statement* for programs able to begin activities in 2023.

Overview:

Priority Regions:

SOIs focused globally or focused on any region will be considered. Applications should prioritize work in Internet-repressive environments.

SOIs regarding technology development should have clear regional human rights use-cases and deployment strategies for the target region(s). SOIs focused on digital safety, advocacy, and research should also have region- or population-specific goals and priorities that are informed by clear field knowledge and expertise.

Internet Freedom Funding Themes:

SOIs **must** address the Goal(s) of one or more of the Internet Freedom Funding Themes: **technology**, **digital safety**, **policy and advocacy**, and **applied research**. Each of the Funding Themes is described in detail below. Applications that do not address the Goals(s) of Funding Themes will not be considered competitive.

Funding Theme-specific guidance and requirements can be found in the following subsections of each Funding Theme: *Goals(s)*; "*Problems of Interest*;" "*To be eligible programs must*;" "*To be eligible programs must NOT*;" and "*Activities that are not typically considered competitive include, but are not limited to*".

Goal(s): The higher-order objectives to which a proposal **must** contribute in order to be eligible for funding under a specific Funding Theme. A strong SOI will include a clear articulation of how the proposed project activities contribute to the Goal(s) of one or more Funding Themes.

Current Problems of Interest *include, but are not limited to*: Problems of interest indicate a subset of current overarching challenges or threats to Internet freedom of notable interest for consideration. SOIs that do not address one or more of these "problems of interest" will **not** be penalized nor disqualified from the competitive process.

To be eligible programs must: A definitive list of the types and methods of activities that proposed programs under a specific Funding Theme MUST meet in order to be eligible for funding. These requirements are in addition to the types and methods of activities outlined in the "*Key Program Considerations*" section that **all programs** MUST include in order to be eligible for funding.

To be eligible programs must NOT: A definitive list of the types and methods of activities that proposed programs under a specific Funding Theme MUST NOT include in order to be eligible for funding. These requirements are in addition to the types and methods of activities outlined in the similarly titled subsection under "*Key Program Considerations*" that **all programs** MUST NOT include in order to be eligible for funding.

Activities that are not typically considered competitive include, but are not limited to: Guidance on the types of activities that previous panels have NOT typically considered competitive. While a SOI will not be immediately excluded from consideration if it contains elements identified in this subsection, it is unlikely to

receive a panel's recommendation for a full proposal. This guidance is provided in addition to the guidance outlined in the similarly titled subsection under "*Key Program Considerations*" which applies to **all programs**.

Funding Theme #1: Technology:

Goal(s): Develop, improve, and implement technologies to support uncensored and secure access to the global Internet and/or to support the goals of other Funding Themes outlined below.

Current Problems of Interest *include, but are not limited to:*

1. *Advanced surveillance, censorship, filtering, or blocking of websites or online services;*
2. *Internet shutdowns, degradation of access;*
3. *Splintering of the Internet;*
4. *The repressive use of spyware, especially when used against civil society, human rights defenders, or independent media.*

To be eligible programs ***must****:*

1. Be based on existing and proven open-source technologies, which have matured to the point where they can be responsibly used in relevant repressive, fragile, or conflict-affected environments and with identified at-risk, marginalized, or vulnerable populations.
2. Serve a clear human rights use case in their application.
3. Demonstrate a clear understanding of adversarial efforts that may impact the use of a proposed technology, and provide a strategy for addressing them.
4. Clearly justify and support specific technical claims and justify their contribution to outcomes related to the Goal(s) of identified Funding Theme(s) (e.g. what specific technologies, protocols, etc. are being used; why a specific technology is being used instead of others; how the technology works to address specific identified threats; etc.)
5. Submit technologies to an independent third-party security audit, according to DRL guidelines.

To be eligible programs **must not**:

1. Be a closed-source technology project (published under proprietary licenses prohibiting code reuse or adaptation).
2. Propose the development of conceptual or aspirational technology without an existing user base or clear application for protecting human rights online.
3. Implement technologies that lack appropriate security for relevant at-risk populations.

*Activities that are **not** typically considered competitive include, but are not limited to:*

1. Technology aiming to support uncensored and secure access to the global Internet that does not address specific repressive threats faced by the populations served and lacking detail describing how the technology will address those threats.
2. Core or surge server infrastructure and/or bandwidth resources for anti-censorship technology.
3. Expansion of physical Internet infrastructure, overcoming fundamental barriers to Internet access (i.e., the physical availability and inherent quality of network connections independent of deliberate government interference or targeted repression).
4. Incorporation of digital technologies (e.g. artificial intelligence, blockchain, virtual reality) without a clear strategic application for, and focus on, protecting human rights **online**.
5. Support for aspirational technologies that have not advanced beyond the proof-of-concept stage, unless those technologies are developed to research or respond to an emergent threat to Internet freedom.
6. Implementation of technologies that a) do not clearly address the unique needs, challenges, and use cases of their target populations; b) do not reflect demand-driven development, or c) fail to incorporate input from local communities.
7. Technology aimed at introducing curated content into censored markets.

Funding Theme #2: Digital Safety:

Goal(s): Conduct programs that enable at-risk, vulnerable, and marginalized populations, or those who protect them, to prepare for, prevent, identify, investigate, and/or obtain remedy for repressive digital attacks; or other types of repression (including online surveillance and censorship) designed to prevent these populations from exercising their human rights and fundamental freedoms online.

***Current Problems of Interest** include, but are not limited to:*

1. *The repressive use of spyware, especially when used against civil society, human rights defenders, or independent media.*
2. *Denial of service (DoS) attacks targeting human rights defenders, independent media and civil society, impacting freedom of expression.*
3. *Digital transnational repression.*

*To be eligible programs **must**:*

1. Have a clear focus on protecting human rights online.

2. Demonstrate a clear understanding of adversarial efforts and a strategy for addressing them.
3. Address acute repressive threats faced by the populations served.
4. Exhibit a clear understanding of the operational risks of operating in local contexts.
5. Clearly demonstrate strong internal capacity and deep expertise in risk management and operational security, with a history of successful implementation of similar programs in high-risk environments.

*To be eligible programs **must not**:*

1. Recommend or implement technology that cannot be safely and responsibly used in relevant repressive, fragile, or conflict-affected environments and with identified at-risk, marginalized, or vulnerable populations.
2. Fail to specify security training methodologies that will be deployed.
3. Conduct generalized "digital literacy" training without a clear impact that improves security for beneficiaries.
4. Contain activities that focus on moderating and/or countering online content unless they explicitly restrict their efforts to only use methods that do not curtail freedom of expression (such as online self-regulation by users, privacy protection measures, etc.).
5. Focus on countering remote offline surveillance.

*Activities that are **not** typically considered competitive include, but are not limited to:*

1. Projects broadly aimed at countering efforts to restrict human rights and fundamental freedoms that are not clearly focused on the online exercise of those rights or freedoms.
2. Digital security education or capacity-building programs not in response to a) a clearly articulated and real threat; b) a specific recent or predicted upcoming change in threat landscapes for the target population; or c) a previously unserved at-risk community.
3. The creation of new generalized security educational or informational security resources primarily containing topical content that is commonly found in resources aimed at the general public.
4. The provision of educational or informational resources exclusively to program participants and not made available for sharing, reuse, revision, or adaptation by other relevant communities and protection providers.
5. Purchases of bulk hardware or bulk licenses for commercial encryption or technology products. In order to be competitive, programs that provide beneficiaries with equipment or services should be discreet efforts that reduce the risk or impact of a) digital attack(s) beneficiaries have recently experienced or b) specific near-term threat(s) beneficiaries are likely to face.

<u>Funding Theme #3</u>: Policy and Advocacy:

Goal(s): Conducting or enabling policy advocacy to counter laws, judicial actions, regulations, standards, company policies, and protocols that restrict human rights and fundamental freedoms online; enabling the Goals of the Digital Safety or Technology Funding Themes; and/or otherwise promote and expand Internet freedom.

Current Problems of Interest *include, but are not limited to:*

1. *Internet shutdowns, including degradation of access.*
2. *Splintering of the Internet.*
3. *Policy or legal measures that restrict human rights and fundamental freedoms online in the guise of promoting cybersecurity or countering cybercrime, disinformation, defamation, hate speech.*
4. *Digital transnational repression.*

To be eligible programs **must**:

1. Clearly identify and articulate a specific Internet freedom policy focus area for advocacy.
2. Demonstrate a clear advocacy strategy, clearly enumerating activities, and setting concrete goals and outcomes for policy change.
3. Articulate a clear understanding of the local policy advocacy context.
6. Exhibit a clear understanding of the operational risks for operating in local contexts.

To be eligible programs **must NOT**:

1. Address digital technology policies or regulations that are not focused on, or without clear direct implications for, the protection of human rights and fundamental freedoms on the global Internet.

Activities that are **not** typically considered competitive include, but are not limited to:

1. Projects focused on digital technologies (e.g. artificial intelligence, blockchain, virtual reality) without a clear strategic application for and focus on protecting human rights **online**.
2. Core support for advocacy capacity development that does not facilitate or support locally-appropriate and locally-led advocacy benefiting local members of civil society or marginalized, vulnerable, and at-risk communities.
3. Advocacy engagements that target U.S. Government stakeholders or allies to promote research findings.

Funding Theme #4: Applied Research:

Goal(s): Research efforts to inform and benefit Internet freedom globally as outlined in the Goal(s) of the above Funding Themes, or to otherwise better understand and counter threats to Internet freedom.

Current Problems of Interest *include, but are not limited to:*

1. *The repressive use of spyware, especially for surveillance, censorship, or repression of civil society, human rights defenders, or independent media.*
2. *Internet shutdowns, degradation of access, and splintering of the Internet.*
3. *Laws, regulations, policies, practices, and protocols that restrict Internet freedom.*
4. *Mitigating the impacts of online abuse and harassment without curtailing freedom of expression.*
5. *Denial of service (DoS) attacks targeting human rights defenders, independent media and civil society, impacting freedom of expression.*

To be eligible, Applied Research programs ***must****:*

1. Have a clear and immediate Internet freedom Policy and Advocacy, Digital Safety, or Technology application.
2. Exhibit a clear understanding of the operational risks for operating in local contexts.
3. Show that they are complementary to, and not duplicative of, existing research.
4. Be transparent in their research methodologies to allow verification, peer review, and further research by others.

To be eligible, Applied Research programs ***must not****:*

1. Conduct purely academic research with no immediate application to protect Internet freedom for specific marginalized, vulnerable, or at-risk populations.
2. Conduct theoretical exploration of technology and/or security issues that does not clearly address a specific articulated threat to Internet Freedom.
3. Conduct experiments on marginalized, vulnerable, at-risk, or actively targeted populations.

Activities that are ***not*** *typically considered competitive include, but are not limited to:*

1. Research scopes that do not indicate a strong baseline understanding of the issue areas.
2. Data/information collection, monitoring, or mapping activities that cannot clearly articulate how the research under their project is complementary to, and/or different from,

existing data/information collection, mapping, and tracking projects, and are not contributing, collaborating, and/or partnering with those existing projects.

3. The use of social-media monitoring tools or other wide-scale collection of personal data without informed consent unless the project can show a clear dedication and capacity to do so responsibly; a robust technical and operational framework for ensuring the safety and privacy of those being monitored; and a compelling case for why this approach is more useful, and would yield more relevant information, than more straightforward research methods that require informed consent.
4. Research within technology, policy, or digital security programs that does not clearly contribute to the project's identified objectives, outcomes, and/or goals.
5. Projects that do not intend to make their research methodology, data, and/or research results freely and publicly available and accessible without having provided compelling potential security, legal, privacy, ethical, or technical justifications.
6. Research that does not show consideration to how its release might positively and negatively interact with fragile or high-risk local contexts or otherwise impact local human lives and interests.
7. Data/information collection, monitoring, or mapping activities that do not show a plan for ensuring longer-term sustainability of the resources created under the project.

Key Program Considerations:

The following list of program considerations is provided as a guide to help applicants develop responsive, robust program proposals.

1. Projects should have a model for long-term **sustainability** beyond the life of the grant.
2. Preferences will be given to projects that create communities of practice and expertise, which do not just include, but elevate, stakeholders from local communities
3. DRL encourages applicants to foster **collaborative partnerships**, especially with local organization(s) in target countries and/or regions, where applicable. Where appropriate, applicants are invited to form consortia for submitting a combined proposal, with one lead ("prime") applicant.
4. DRL strongly encourages applicants to consider contributing to, enhancing, collaborating or partnering with the developers of, and/or updating existing similar research, educational materials, or other resources before creating duplicative or similar products.
5. When working with marginalized and vulnerable populations, preference will be given to projects that substantively partner with organizations or groups that are composed of, or led by, members of the populations being supported and/or explicitly focus on issues related to those groups.

6. DRL strives to ensure its programs advance the rights and uphold the dignity of the most **at-risk and vulnerable populations**. Projects that directly engage with or focus on such groups, or with activities in repressive environments, must show an understanding of context-specific ethical and safety considerations of their approach, a clear plan for responsibly and safely conducting their work, and appropriate capacity and expertise to carry out that plan and respond to emergent risks to the program, implementers, and/or beneficiaries.
7. Any development or use of Artificial Intelligence and/or Machine Learning will be required to comply with Executive Order (E.O) 1396's 9 Principles for Use of AI in Government.
8. All peer-reviewed scholarly publications authored or coauthored by individuals or institutions resulting from research conducted under proposed programs must be made freely and publicly available and accessible by default without any embargo or delay after publication, in accordance with administration policy. Research projects will be required to provide significant justification and approval for any restrictions or limitations on data access, use, and disclosure.

*To be eligible ALL programs **must**:*

1. Clearly address one or more of the above Internet Freedom Funding Themes.

*To be eligible ALL programs **must not**:*

1. Focus on digital technologies (e.g. algorithmic tools, blockchain, virtual reality, Internet of Things, facial recognition) without a clear strategic application for and focus on protecting human rights **online**.
2. Contain activities that focus on moderating and/or countering online content unless they explicitly restrict their efforts to only use methods which do not curtail freedom of expression (such as online self-regulation by users, privacy protection measures, etc.).
3. Contain offensive cybersecurity efforts, such as hacking, or counter-attacking.

*Programs and activities that are **not** typically considered competitive within ANY program theme, include, but are not limited to*

1. Activities that go beyond an organization's demonstrated competence, or for which the applicant does not show evidence of their ability to safely and responsibly carry out those activities and achieve the stated impact;
2. Projects without a real-world impact that improves Internet Freedom in specific countries or regions.

3. Geographically or community focused programs that do not articulate how their strategies clearly address or are tailored for the unique needs, risks, challenges, use cases, and cultural contexts of their target populations.
4. Programs in repressive, fragile, or conflict-affected environments and/or targeting at-risk, marginalized, or vulnerable populations that do not show clear consideration for how the context may impact the program's efforts and how the program may positively and negatively change the local context and otherwise impact local human lives and interests.
5. The use of social-media monitoring tools or other wide-scale collection of personal data without informed consent. Projects proposing this must be able to show a clear dedication and capacity to do so responsibly; a robust technical and operational framework for ensuring the safety and privacy of those being monitored; and a compelling case for why this approach is more useful, and would yield more relevant information, than more straightforward research methods that require informed consent.
6. Projects that focus on expansion of physical Internet infrastructure or overcoming first-order barriers to Internet access (i.e., the physical availability and inherent quality of network connections independent of deliberate government interference or targeted repression).
7. The creation of new educational or informational resources that cannot clearly articulate how they are complementary to, and not duplicative of, other similar current and previous efforts. Projects that cannot do this must provide significant justification for why they could not build on, contribute back to, revive, update, translate, or localize existing resources to serve their purposes.
8. Projects that aim to establish, produce, or create resources, technology, research efforts, service delivery mechanisms, or networks *that are intended to continue to be utilized beyond the life of the project* without including tangible efforts within the project design to ensure this sustainable continuity.
9. Projects that do not intend to make resources, technologies, and/or research findings they produce freely and publicly available and accessible. These projects must provide compelling potential security, legal, privacy, ethical, or technical justification for restricting their availability.
10. Projects that focus on a single country rather than a regional or global approach.
11. Stand-alone public awareness campaigns.
12. Study tours, scholarships or exchange projects.

All programs should aim to have impact that leads to reforms and should have the potential for sustainability beyond DRL resources. DRL's preference is to avoid duplicating past efforts by supporting new and creative approaches. This does not exclude from consideration projects that improve upon or expand existing successful projects in a new and complementary way. Programs should seek to include groups that can bring perspectives based on their religion,

gender, disability, race, ethnicity, and/or sexual orientation and gender identity. Programs should be demand-driven and locally led to the extent possible. DRL requires all programs to be non-discriminatory and expects implementers to include strategies for integration of individuals/organizations regardless of religion, gender, disability, race, ethnicity, and/or sexual orientation and gender identity.

To maximize the impact and sustainability of the award(s) that result(s) from this RSOI/NOFO, DRL reserves the right to execute a non-competitive continuation amendment(s). Any non-competitive continuation is contingent on performance and **availability of funds**. A non-competitive continuation is not guaranteed; the Department of State reserves the right to exercise or not exercise the option to issue non-competitive continuation amendment(s).

II. Eligibility Information

Organizations submitting SOIs must meet the following criteria:

- Be a U.S.- or foreign-based non-profit/non-governmental organization (NGO), or a public international organization; or
- Be a private, public, or state institution of higher education; or
- Be a for-profit organization or business (noting there are restrictions on payment of fees and/or profits under grants and cooperative agreements, including those outlined in 48 CFR 30, "Cost Accounting Standards Administration", and 48 CFR 31, "Contract Cost Principles and Procedures");
- Have existing, or the capacity to develop, active partnerships with thematic or in-country partners, entities, and relevant stakeholders including private sector partner and NGOs; and,
- Have demonstrable experience administering successful and preferably similar programs. DRL reserves the right to request additional background information on organizations that do not have previous experience administering federal awards. These applicants may be subject to limited funding on a pilot basis.

Applicants may **form consortia** and submit a combined SOI. However, one organization should be designated as the lead applicant with the other members as sub-award partners.

DRL's preference is to work with **non-profit** entities; however, there may be some occasions when a for-profit entity is best suited. Applications submitted by for-profit entities may be subject to additional review following the panel selection process. Additionally, the Department of State prohibits profit to for-profit or commercial organizations under its assistance awards. Profit is defined as any amount in excess of allowable direct and indirect costs. The allowability of costs incurred by commercial organizations is determined in accordance with the provisions of the Federal Acquisition Regulation (FAR) at 48 CFR 30, Cost Accounting Standards Administration, and 48 CFR 31 Contract Cost Principles and Procedures. Please see 2 CFR 200.307 for regulations regarding program income.

DRL is committed to an **anti-discrimination policy** in all of its programs and activities. DRL welcomes SOI submissions irrespective of race, ethnicity, color, creed, national origin, gender, sexual orientation, gender identity, disability, or other status.

Any applicant listed on the Excluded Parties List System in the System for Award Management (SAM.gov) (www.sam.gov) and/or has a current debt to the U.S. government is not eligible to apply for an assistance award in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR,1986 Comp., p. 189) and 12689 (3 CFR,1989 Comp., p. 235), "Debarment and Suspension." Additionally, no entity or person listed on the Excluded Parties List System in SAM.gov can participate in any activities under an award. All applicants are strongly encouraged to review the Excluded Parties List System in SAM.gov to ensure that no ineligible entity or person is included in their application.

Organizations are not required to have a valid Unique Entity Identifier (UEI) number—formerly referred to as a DUNS (Data Universal Numbering System) number—and an active SAM.gov registration to apply for this solicitation through SAMS Domestic. **However, if a SOI is approved, these will need to be obtained before an organization is able to submit a full application. Therefore, we recommend starting the process of obtaining a UEI and SAM.gov registration as soon as possible.** Please note that there is no cost associated with UEI or SAM.gov registration.

III. Application Requirements, Deadlines, and Technical Eligibility

All SOIs must conform to DRL's posted Proposal Submission Instructions (PSI) for Statements of Interest, as updated in November 2021, available at https://www.state.gov/bureau-of-democracy-human-rights-and-labor/programs-and-grants/.

Complete SOI submissions **must** include the following:

1. Completed and signed SF-424 and SF424B, as directed on SAMS Domestic or Grants.gov (please refer to DRL's PSI for SOIs for guidance on completing the SF-424); and,
2. Program Statement (not to exceed three (3) pages in Microsoft Word) that includes:
    a) A table listing:
        i. Name of the organization;
        ii. The target country/countries;
        iii. The total amount of funding requested from DRL, total amount of cost-share (if any), and total program amount (DRL funds + cost-share); and,
        iv. Program length;
    b) A synopsis of the program, including a brief statement on how the program will have a demonstrated impact and engage relevant stakeholders. The SOI should identify local partners as appropriate;
    c) A concise breakdown explicitly identifying the program's objectives and the activities and expected results that contribute to each objective; and,

d) A brief description of the applicant(s) that demonstrates the applicant(s) expertise and capacity to implement the program and manage a U.S. government award.

Primary organizations can submit 2 SOIs in response to the RSOI. If an applicant chooses to submit multiple applications to this RSOI, it is the responsibility of the applicant to demonstrate the competitiveness and uniqueness of each SOI. **SOIs that request less than $500,000 or more than $3,000,000 may be deemed technically ineligible.**

Technically eligible SOIs are those which:

1) Arrive electronically via SAMS Domestic or Grants.gov by **11:59 PM EST on January 13, 2023 the announcement titled "DRL FY22 Internet Freedom Annual Program Statement Round 2," funding opportunity number SFOP0009225**
2) Are in English;
3) Heed all instructions and do not violate any of the guidelines stated in this solicitation and the PSI for Statements of Interest.

For all SOI documents please ensure:

1) All pages are numbered;
2) All documents are formatted to 8 ½ x 11 paper; and,
3) All documents are single-spaced, 12-point Times New Roman font, with 1-inch margins. Captions and footnotes may be 10-point Times New Roman font. Font sizes in charts and tables can be reformatted to fit within one page width.

Grants.gov and SAMS Domestic automatically log the date and time an application submission is made, and the Department of State will use this information to determine whether an application has been submitted on time. Late applications are neither reviewed nor considered. Known system errors caused by Grants.gov or SAMS Domestic (https://mygrants.service-now.com) that are outside of the applicant's control will be reviewed on a case by case basis. Applicants should not expect a notification upon DRL receiving their application. DRL will **not** accept SOIs submitted via email, fax, the postal system, delivery companies, or couriers. DRL strongly encourages all applicants to submit SOIs before January 13, 2023to ensure that the SOI has been received and is complete.

IV. Review and Selection Process

DRL strives to ensure that each application receives a balanced evaluation by a DRL review panel. The Department's Office of Acquisitions Management (AQM) will determine technical eligibility for all SOI submissions. All technically eligible SOIs will then be reviewed against the same four criteria by a DRL Review Panel: quality of program idea, addressing barriers to equal participation, program planning, and ability to achieve objectives/institutional capacity.

Additionally, the Panel will evaluate how the SOI meets the solicitation request, U.S. foreign policy goals, and DRL's overall priority needs. Panelists review each SOI individually against

the evaluation criteria, not against competing SOIs. To ensure all SOIs receive a balanced evaluation, the DRL Review Panel will review the first page of the SOI up to the page limit and no further. All Panelists must sign non-disclosure agreements and conflict of interest agreements.

In most cases, the DRL Review Panel includes representatives from DRL policy and program offices. Once a SOI is approved, selected applicants will be invited to submit full proposal applications based on their SOIs. Unless directed otherwise by the organization, DRL may also refer SOIs for possible consideration in other U.S. government related funding opportunities.

The Panel may provide conditions and/or recommendations on SOIs to enhance the proposed program, which must be addressed by the organization in the full proposal application. To ensure effective use of limited DRL funds, conditions and recommendations may include requests to increase, decrease, clarify, and/or justify costs and program activities.

DRL's Front Office reserves the right to make a final determination regarding all funding matters, pending funding availability.

Review Criteria

Quality of Program Idea

SOIs should be responsive to the program framework and policy objectives identified in the RSOI, appropriate in the country/regional context, and should exhibit originality, substance, precision, and relevance to DRL's mission of promoting human rights and democracy. Projects should have the potential to have an immediate impact leading to long-term, sustainable reforms. DRL prefers new approaches that do not duplicate efforts by other entities. This does not exclude from consideration projects that improve upon or expand existing successful projects in a new and complementary way. In countries where similar activities are already taking place, an explanation should be provided as to how new activities will not duplicate or merely add to existing activities and how these efforts will be coordinated. SOIs that promote creative approaches to recognized ongoing challenges are highly encouraged. DRL prioritizes project proposals with inclusive approaches for advancing these rights.

Addressing Barriers to Equal Participation

DRL strives to ensure its projects advance the rights and uphold the dignity of all persons. As the U.S. government's lead bureau dedicated to promoting democratic governance, DRL requests a programming approach dedicated to strengthening inclusive societies as a necessary pillar of strong democracies. Violence targeting any members of society undermines collective security and threatens democracy. DRL prioritizes inclusive and integrated program models that assess and address the barriers to access for individuals and groups based on their religion, gender, disabilities, ethnicity, or sexual orientation and gender identity. Applicants should describe how programming will impact all of its beneficiaries, including support that specifically targets communities facing discrimination, and which may be under threat of violence.

Program Planning
A strong SOI will include a clear articulation of how the proposed program activities and expected results (both outputs and outcomes) contribute to specific program objectives and the overall program goal. Objectives should be ambitious, yet measurable, results-focused, and achievable in a reasonable time frame.

Ability to Achieve Objectives/Institutional Capacity
SOIs should address how the program will engage relevant stakeholders and should identify local partners as appropriate. If local partners are identified, applicants should describe the division of labor among the applicant and any local partners. SOIs should demonstrate the organization's expertise and previous experience in administering programs, preferably similar programs targeting the requested program area or similarly challenging environments.

For additional guidance, please see DRL's posted Proposal Submission Instructions (PSI) for Statements of Interest, as updated in November 2021, available at https://www.state.gov/proposal-submission-instructions/.

V. Additional Information

DRL will not consider applications that reflect any type of support for any member, affiliate, or representative of a designated terrorist organization. Please refer the link for Foreign Terrorist Organizations: https://www.state.gov/foreign-terrorist-organizations/. Project activities whose direct beneficiaries are foreign militaries or paramilitary groups or individuals will not be considered for DRL funding given purpose limitations on funding.

In accordance with Department of State policy for terrorism, applicants are advised that successful passing of vetting to evaluate the risk that funds may benefit terrorists or their supporters is a condition of award. If chosen for an award, applicants will be asked to submit information required by DS Form 4184, Risk Analysis Information (attached to this solicitation) about their company and its principal personnel. Vetting information is also required for all sub-award performance on assistance awards identified by the Department of State as presenting a risk of terrorist financing. Vetting information may also be requested for project beneficiaries and participants. Failure to submit information when requested, or failure to pass vetting, may be grounds for rejecting your proposal prior to award.

The Leahy Law prohibits Department foreign assistance funds from supporting foreign security force units if the Secretary of State has credible information that the unit has committed a gross violation of human rights. Per 22 USC §2378d(a) (2017), "No assistance shall be furnished under this chapter [FOREIGN ASSISTANCE] or the Arms Export Control Act [22 USC 2751 et seq.] to any unit of the security forces of a foreign country if the Secretary of State has credible information that such unit has committed a gross violation of human rights." Restrictions may apply to any proposed assistance to police or other law enforcement. Among these, pursuant to section 620M of the Foreign Assistance Act of 1961, as amended (FAA), no assistance provided through this funding opportunity may be furnished to any unit of the security forces of a foreign country when there is credible information that such unit has committed a gross violation of

human rights. In accordance with the requirements of section 620M of the FAA, also known as the Leahy law, project beneficiaries or participants from a foreign government's security forces may need to be vetted by the Department before the provision of any assistance. If a proposed grant or cooperative agreement will provide assistance to foreign security forces or personnel, compliance with the Leahy Law is required.

Organizations should be aware that DRL understands that some information contained in SOIs may be considered sensitive or proprietary and will make appropriate efforts to protect such information. However, organizations are advised that DRL cannot guarantee that such information will not be disclosed, including pursuant to the Freedom of Information Act (FOIA) or other similar statutes.

Organizations should also be aware that if ultimately selected for an award, DRL requires all recipients of foreign assistance funding to comply with all applicable Department and Federal laws and regulations, including but not limited to the following: The Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards set forth in 2 CFR Chapter 200 (Sub-Chapters A through F) shall apply to all non-Federal entities, except for assistance awards to Individuals and Foreign Public Entities. Sub-Chapters A through E shall apply to all foreign organizations, and Sub-Chapters A through D shall apply to all U.S. and foreign for-profit entities. The applicant/recipient of the award and any sub-recipient under the award must comply with all applicable terms and conditions, in addition to the assurance and certifications made part of the Notice of Award. The Department's Standard Terms and Conditions can be viewed at https://www.state.gov/about-us-office-of-the-procurement-executive/.

The information in this solicitation and DRL's PSI for SOIs, as updated in November 2021, is binding and may not be modified by any DRL representative. **Explanatory information provided by DRL that contradicts this language will not be binding.** Issuance of the solicitation and negotiation of SOIs or applications does not constitute an award commitment on the part of the U.S. government. DRL reserves the right to reduce, revise, or increase proposal budgets in accordance with the needs of the program evaluation requirements.

This solicitation will appear on www.grants.gov, SAMS Domestic (https://mygrants.servicenowservices.com), and DRL's website https://www.state.gov/statements-of-interest-requests-for-proposals-and-notices-of-funding-opportunity/.

Background Information on DRL and DRL Funding

DRL has the mission of promoting democracy and protecting human rights globally. DRL supports programs that uphold democratic principles, support and strengthen democratic institutions, promote human rights, prevent atrocities, combat and prevent violent extremism, and build civil society around the world. DRL typically focuses its work in countries with egregious human rights violations, where democracy and human rights advocates are under pressure, and where governments are undemocratic or in transition.

Additional background information on DRL and the human rights report can be found on https://www.state.gov/bureaus-offices/under-secretary-for-civilian-security-democracy-and-human-rights/bureau-of-democracy-human-rights-and-labor/.

VI. Contact Information

SAMS Domestic Help Desk:
For assistance with SAMS Domestic 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.service-now.com/ilms/home. Customer support is available 24/7.

Please note that establishing an account in SAMS Domestic may require the use of smartphone for multi-factor authentication (MFA). If an applicant does not have accessibility to a smartphone during the time of creating an account, please contact the helpdesk and request instructions on MFA for Windows PC.

Grants.gov Helpdesk:
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.

See https://www.opm.gov/policy-data-oversight/pay-leave/federal-holidays/ for a list of federal holidays.

For technical questions related to this solicitation, please contact InternetFreedom@state.gov.

Except for technical submission questions, during the RSOI period U.S. Department of State staff in Washington and overseas shall not discuss this competition with applicants until the entire proposal review process has been completed and rejection and approval letters have been transmitted.