Department of State
Public Notice

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

I. Requested Objectives for Statements of Interest

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 the policy objective to support Internet Freedom. In support of the U.S. International Strategy for Cyberspace, 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 Grants.gov in order to obtain a username and password. **All SOI submissions must be made electronically via www.grants.gov. Please note that the Grants.gov registration process can take ten (10) business days or longer, even if all registration steps are completed in a timely manner.** For instructions on how to register with Grants.gov 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.

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 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 Funding Themes will not be considered competitive.

Areas of Focus:

Within each of the Internet Freedom funding themes, DRL has identified "Areas of Focus." *SOIs do **not** need to fit into one of these areas to be considered.* They are provided solely to indicate a subset of current areas of interest for consideration. Applications that do not address one or more of these "areas of focus" will **not** be penalized nor disqualified from the competitive process.

Funding Theme #1: Technology: Uncensored and Secure Access to the Global Internet – Development of and support for technologies that counter censorship, enable secure communications, or otherwise protect and strengthen digital safety for human rights defenders. These tools should be tailored to the needs of human rights defenders and the acute and diverse threats they face. The tool design and deployment should be informed by user-centered design and risk assessments that are focused on these communities, and these tools should be supported on the platforms (desktop, mobile, etc.) that these communities most use. Projects may include but are not limited to:

- Development of new technologies for defeating censorship, for maintaining availability of information, for secure communications, for privacy protection, and online services such as email and website hosting with robust defenses against hacking and other attacks.
- Improvements to proven technologies including distribution, expansion, adaptation, and/or localization of proven anti-censorship or secure communication technologies; and improvement of usability and user interfaces to enable broader populations of users to adopt such tools.
- Reusable libraries or protocols to provide the underlying software components that may be used by anti-censorship and secure communication tools.
- Development of critical infrastructure to support an open, interoperable, reliable, and secure internet by implementing privacy-by-design and raising the cost of censorship.

Areas of Focus:

§ Scalable and sustainable next-generation anti-censorship and secure communication technologies, especially for platforms that generally have less support for anti-censorship and secure communication.

§ Alternative production and sustainability models for anti-censorship tools, such as white-label and branded content apps.

§ Development and implementation of alternative methods for distributing software applications in closed or repressive Internet contexts.

§ Development and implementation of protocols and critical infrastructure to support an open, interoperable, reliable, and secure Internet, including through the promotion, adoption, and integration of new or proven circumvention and security protocols in existing technology stacks.

§ Development, improvement, and/or implementation of technologies to enable at-risk individuals, organizations, or communities with limited resources to more easily conduct investigations of digital attacks, or implement improved mitigations and security practices on the basis of threat intelligence and/or guidance shared with them by trusted civil society peers.

§ Development, improvement, and/or implementation of secure technologies that allow human rights defenders to safely use the internet to accomplish critical tasks when their access to connectivity is limited by cost, network availability or coverage, slow network speeds, shutdowns, or outdated technology.

§ Security improvements to enable open-source technologies that could serve critical functional needs of human rights defenders to be safely and effectively used in repressive environments.

Funding Theme #2: Digital Safety – Support, training, and information resources that contribute to greater digital safety for users in Internet-repressive societies, including civil society, human rights defenders, journalists, and other vulnerable populations. Projects may include but are not limited to:

- *Digital safety skills development* for civil society through trainings, organizational security audits, mentorship, local leadership development, peer learning, and guided practice approaches employing adult learning pedagogies.
- *Emergency support* to respond to and prevent future incidents of digital attacks, including the use of targeted hacking, disruption, confiscation of devices, seizure of data, or means to monitor, harass, or repress members of civil society.
- *Resource development and information dissemination* to targeted communities, the general public, or local civil society digital safety experts to raise awareness of digital threats, provide appropriate mitigations and/or defensive strategies, and respond to sudden threats to Internet Freedom.
- *Local and/or regional capacity-building programs* to support non-US based civil society digital safety experts to more effectively educate civil society and identify, investigate,

expose, and take action to protect at-risk and vulnerable groups from repressive digital threats.
- *Regional coalition-building efforts* to expand networks of civil society digital safety experts, increase their coordination, and improve their sustainability.

Areas of Focus:

§ Development of tailored digital safety resources and training methodologies for vulnerable populations, such as journalists and independent media, in places where they are threatened.

§ Holistic and proactive training and skill-building programs that build digital safety capacity in conjunction with physical security and psychosocial care.

§ Programs establishing or strengthening efforts to create and share actionable threat intelligence, mitigations, and defensive strategies among local, regional, and/or international networks of civil society digital safety experts, in order to support more effective digital protection and emergency response support mechanisms.

§ Broad public awareness campaigns to promote digital hygiene and increase the adoption of digital safety tools and practices in highly repressive environments.

§ Initiatives that raise awareness of the digital threats that human rights defenders, journalists, and other targeted communities face and provide guidance on effective defenses and deterrents against those threats.

Funding Theme #3: Policy and Advocacy – National, regional, and international policy and advocacy efforts that empower civil society to counter restrictive Internet laws and support policies to promote Internet Freedom in countries where the government has adopted, or is considering adopting, laws or policies that restrict human rights online. Projects may include but are not limited to:

- *Local capacity-building* programs to support the development of non-U.S. based civil society organizations to advocate for human rights online.
- *Regional coalition-building* efforts to expand networks, increase coordination, and develop regional standards that protect and promote Internet Freedom.
- *International engagement* opportunities to increase civil society participation in international policy dialogues, support multi-stakeholder engagement, and promote Internet Freedom at key international fora.

Areas of Focus:

§ Initiatives to mainstream Internet Freedom and online human rights standards into regional and international cyber policy-making processes and dialogues.

§ Initiatives to institutionalize Internet policy and advocacy expertise in local law firms, legal institutions, and law schools that will support specific, localized, and impactful policy and legal advocacy efforts.

§ Initiatives to enhance coordination and exchanges between policy advocates and technologists.

§ Advocacy targeting technology companies and developers, addressing the privacy, freedom of expression, and freedom of association rights of vulnerable groups using new technologies.

§ Programs that support the capacity and efforts of local civil society in developing countries to engage more directly with large, established, and market-dominant technology companies, especially in the global north, to raise awareness of their impacts on human rights in those contexts and advocate for accountability and change.

§ Programs that promote accountability and remedy through identification, exposure of, and engagement with companies complicit in supplying and/or supporting network and/or online surveillance that adversely impacts, restricts, or violates the human rights of online users to privacy or the freedoms of expression, assembly, or association.

§ Advocacy efforts that promote the adoption of infrastructure and protocols that inherently protect user privacy and raise the cost of censorship, especially within international standards-setting bodies.

§ Advocacy targeting technology companies, developers, policy makers and/or judicial systems to improve the ability of victims of repressive cyber attacks to access and use evidence to hold perpetrators accountable, obtain remedy, and/or aid in identifying, preventing, or mitigating attacks against other possible targets.

§ Initiatives to ensure global norms and standards relevant to the use or prohibition of online and network surveillance incorporate Internet Freedom and human rights values concerning privacy and freedom of expression.

Funding Theme #4: Applied Research – Research efforts to inform and benefit Internet Freedom globally. Research should address technological and political developments affecting Internet Freedom. Projects may include but are not limited to:

- *Real-time monitoring and analysis* of both technical and policy threats to Internet Freedom. Global assessments of Internet Freedom threats, opportunities, and trends.

- *Policy research and legal analysis* to increase awareness of Internet policy trends and enhance targeted national, regional, or international advocacy efforts.
- *Technical research and analysis* into the design, development, and deployment of existing or developing online technologies, to identify and increase awareness of the risks, vulnerabilities, threats, and impacts for human rights online.

Areas of Focus:

§ Initiatives that develop and share actionable threat information on the ongoing and emerging tactics, techniques, and procedures used by governments to conduct digital repression of civil society and human rights defenders.

§ Assessments of technological best practices and the current state of play of anti-censorship and secure communication tools and techniques to inform the Internet Freedom technical community, and improve approaches to anti-censorship and secure communication.

§ Online censorship analyses that aggregate and list blocked items, terms, or websites, for the purposes of censorship tracking, and potential content re-introduction.

§ Assessments of the political, legal, and technical factors that enable Internet shutdowns or throttling in various contexts, and recommendations for responding to, mitigating, and preventing shutdowns.

§ Programs that explore the implications and impacts of Internet network architecture design (including, but not limited to, Tier 1 providers, cloud service providers, and internet service providers) for Internet Freedom and human rights online, including the fragility, inherent vulnerabilities, or ease of abuse of such architecture.

§ Cyber-threat intelligence collection and analysis, including data forensics, and information sharing to support human rights defenders and civil society.

§ Programs that improve the ability of victims of repressive cyber attacks to get access to evidence of those abuses and use them to hold perpetrators accountable, seek remedy, and aid in identifying, preventing, or mitigating attacks against other possible targets.

§ Research on measures to mitigate against the impacts of online abuse and harassment, without curtailing freedom of expression (such as online self-regulation by users, privacy protection measures, etc.).

§ Retrospective research to identify relationships between the design, development, management, or business and revenue models of technologies and online services, and the

human rights impacts of those decisions on vulnerable, marginalized, or targeted user populations.

Key Program Considerations:

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

- Preferences will be given to projects consistent with DRL's approach to supporting sustainable **open-source technical projects.** Internet Freedom projects should have a model for long-term **sustainability** beyond the life of the grant.
- 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.
- DRL strives to ensure its programs advance the rights and uphold the dignity of the most **at-risk and vulnerable populations**. Projects which 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.

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 strategies for integration and inclusion of individuals/organizations/beneficiaries that can bring perspectives based on their religion, sex, disability, race, ethnicity, sexual orientation, gender identity, gender expression, sex characteristics, national origin, age, genetic information, marital status, parental status, pregnancy, political affiliation, or veteran's status. 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 nondiscrimination of individuals/organizations/beneficiaries based on race, color, religion, sex, gender identity, gender expression, sex characteristics, sexual orientation, pregnancy, national origin, disability, age, genetic information, marital status, parental status, political affiliation, or veteran's status.

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).

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

- Closed-source technology projects (published under proprietary licenses, prohibiting code reuse or adaptation).
- Academic research with no immediate internet freedom application; theoretical exploration of technology and/or security issues;
- Purchases of bulk hardware or bulk licenses for commercial encryption or technology products;
- Activities that focus on moderating and/or countering online speech. (Including, but not limited to, online propaganda, mis/disinformation, harassment, and/or hate-speech.)
- Technology development or digital safety interventions without a clear human rights use case in an Internet repressive environment, or without a clear threat model and understanding of adversarial efforts;
- Core or surge server infrastructure and/or bandwidth resources for anti-censorship technology;
- Study tours, scholarships or exchange projects;
- Projects that focus on 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);
- Projects that focus on a single country rather than a regional or global approach;
- Stand-alone public awareness campaigns and/or public awareness campaigns not directly tied to one of the four funding categories listed above;
- Projects not sufficiently connected to real-world impact of improving Internet Freedom environments in any country or region;
- Activities that go beyond an organization's demonstrated competence, or for which applicant does not show evidence of the ability to safely and responsibly carry out those activities and achieve the stated impact;
- Projects focused on emerging technologies (e.g. artificial intelligence, blockchain, virtual reality) without a clear focus on protecting human rights online.

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 projects and activities. DRL welcomes applications irrespective of race, ethnicity, color, creed, national origin, gender, sexual orientation, gender identity, disability, or other status. DRL seeks applications that demonstrate that the recipient does not discriminate against any beneficiaries in implementation of a potential award, such as, but not limited to, by withholding, adversely impacting, or denying equitable access to the benefits provided through this award on the basis of any factor not expressly stated in the award. This includes, for example, race, color, religion, sex (including gender identity, gender expression, sex characteristics, sexual orientation, and pregnancy), national origin, disability, age, genetic information, marital status, parental status, political affiliation, or veteran's 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 grants.gov. **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 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 Grants.gov by 11:59 PM EST on March 11, 2022 under the announcement titled "DRL FY22 Internet Freedom Annual Program Statement," funding opportunity number SFOP0008485**;
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 automatically logs 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 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 **March 11, 2022** to 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. Discrimination, violence, inequity, and inequality 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 race, ethnicity, religion, income, geography, gender identity, sexual orientation, or disability. The SOI should also demonstrate how the program will further engagement in underserved communities and with individuals from underserved communities. Applicants should describe how programming will impact all of its beneficiaries, including support for underserved and underrepresented communities. Stakeholders shall identify the difference between opportunities and barriers to access, and design programs accordingly to not perpetuate these inequalities, but rather enhance programmatic impact by including all people in society. The goal of this approach is to bring communities and those in power together in support of more stable and secure societies.

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

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.