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.

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.

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.

Funding Themes

Funding Theme #1: Technology: Uncensored and Secure Access to the Global Internet – Development of and support for desktop and mobile technologies that counter censorship and/or enable secure communications. 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 that is 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.
- Re-usable 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 increasing 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.
- Next-generation malware detection and mitigation systems.
- Alternative production and sustainability models for anti-censorship tools, such as whitelabel 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.

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 urgent cases and to prevent future digital attacks, including harassment and violence against individuals in retribution for their online activities.

- Resource development and information dissemination to targeted communities, or the general public, to raise awareness of digital threats, encourage best practices, and respond to sudden threats to Internet freedom.

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 to build the capacity of local digital safety trainers and foster regional training networks and training opportunities.
- Programs to establish or strengthen emergency response mechanisms by integrating and sharing cyber threat intelligence analysis and research through networks and Cyber Incident and Emergency Response Teams.
- Broad public awareness campaigns to promote digital hygiene and increase the adoption of digital safety tools and practices in highly repressive environments.
- Initiatives that promote and raise awareness on the safe and secure use of social media for human rights defenders, journalists, and other targeted communities.
- Projects that develop, expand, and implement both proven and innovative support resources and methodologies to Hong Kong, Mexico and/or other countries across Latin America and the Caribbean.

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 to support policies that protect and promote Internet freedom.
- International engagement opportunities to increase civil society participation in international policy dialogues to support multi-stakeholder engagement and promote Internet freedom at key international for a

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 training and expertise in local law firms, legal institutions, and law schools.
- 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 integrate stakeholders involved in the development and implementation of critical infrastructure and secure protocols into policy advocacy efforts. Advocacy efforts should promote the adoption of infrastructure and protocols that inherently protect user privacy and raise the cost of censorship, especially in international standards-setting bodies.
- Advocacy efforts to integrate human right considerations into the development of policies related to emerging technologies (e.g. artificial intelligence).

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.

Areas of Focus

- Cyber-threat intelligence collection and analysis, including data forensics, and information sharing to support human rights defenders and civil society.
- Assessments of technological best practices and the current state of play of anticensorship and secure communication tools and techniques to inform the Internet freedom technical community and improve approaches to anti-censorship and secure communication.
- Online censorship analysis that aggregates and lists blocked items, terms, or websites, for the purposes of censorship tracking, and potential content re-introduction.
- Assessments of the political, legal or regulatory, and technical factors that enable and Internet shutdowns or throttling in various contexts and recommendations for responding to, mitigating, and preventing shutdowns
- Assessments of the human rights implications and impacts of—as well as considerations that should inform—emerging technologies, including but not limited to artificial intelligence (AI) and Internet of Things (IoT) technologies.

Funding Information

- **Award Ceiling:** $3,000,000
- **Award floor:** $ 5,00,000

Eligibility Criteria

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”); and
- 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.

For more information, visit Grants.gov.