The Rapid Response Fund aims to resolve threats in a timely and comprehensive manner for individuals, communities, and organizations whose free expression has recently been repressed. To resolve digital emergencies, OTF offers both direct financial support as well as technical services from trusted partners to high-risk people and organizations, such as bloggers, cyber activists, journalists, and human rights defenders.

Setting the stage

The Rapid Response Fund offers two types of support to organizations, activists, journalists, and other human rights defenders facing digital attacks and emergencies of various kinds:

1. technological services from trusted service partners and
2. direct financial support for the many needs that cannot be fulfilled by available service partners.

For either form of support, the process starts with a single application. Support is only available through the Rapid Response Fund when there is a **clear and time-sensitive** digital emergency in which an applicant is seeking short-term and urgent support.

The Rapid Response Fund does not provide support for projects that are long-term in nature or that aim to build digital security capacity among groups or organizations. If you are interested in receiving support for longer term capacity building, please consider applying to OTF's Internet Freedom Fund. We have also compiled a list of alternative sources of support for Rapid Response and digital security initiatives here.

Trusted Partners

We work exclusively with community partners who are highly sensitive to and well-aware of the specific needs and challenges of human rights activists, journalists, and the Internet

freedom community. These partners regularly work with individuals and organizations who are subject to repressive regimes or vulnerable to malicious censorship and surveillance. To respond to requests as quickly as possible, OTF maintains open agreements with these partners to provide the following services.

Tierra Comun can provide the following services:

Organizational Security & Digital Security Support including:

1. Digital security audits for organizations
2. Urgent risk mitigation for organizations
3. Rapid assessment and crisis response planning for organizations
4. Organizational security improvements
5. Digital security mentoring

Languages supported by Tierra Comun:

- English
- Spanish

Contact Information

Please reach out to this dedicated address for receiving and managing orders: infosec@tierracomun.org

Greenhost can provide the following services:

Web Hosting including:

- Clustered web hosting
- Cloud platform
- Deflect anti-DDoS protection

- Infrastructure as a Service (IAAS)
- Real-time Monitoring

Languages supported by Greenhost:

- English
- Arabic
- French
- Spanish
- Mandarin

Contact Information

Please reach out to this dedicated address for rapid response requests: rr@greenhost.net

Qurium Media Foundation can provide the following services:

Organizational Security & Digital Security Support

Support including:

- Digital security audits for organizations
- Urgent risk mitigation for organizations
- Rapid assessment and crisis response planning for organizations
- Organizational security improvements
- Digital security mentoring

Digital Attacks Response & Forensic Analysis

Analysis including:

- Analysis of malicious mobile apps
- Security Audits of web applications and systems
- Forensic analysis of digital attacks
- Recovery of compromised websites
- Audit of compromised websites
- Malware analysis

- DDoS response and mitigation
- Web application and website vulnerability assessments
- Analysis of compromised mobile phones

Web Hosting including:

- Migration and onboarding support
- Secure web hosting
- Secure hosting, monitoring, and resiliency of websites during special events (elections, campaigns etc.)
- Provision of human rights abuse documentation tools
- Enabling access to blocked websites (e.g. website mirroring)

Connectivity Issues Response including:

- Establishing VPN servers during digital emergencies
- Providing internet access alternatives during shutdowns/censorship events
- Analysis of Internet disruption events
- Network shutdown response

Languages supported by Qurium Media Foundation:

- English
- Spanish
- French
- Russian
- Arabic
- Swedish

Contact Information

The application form for Qurium Media Foundation is available here.

Direct Financial Support

When rapid response applicants' needs are not sufficiently covered by our service partners, OTF can provide financial support directly to activists, journalists and related organizations to help prepare for or mitigate digital threats or emergencies, given applicants can demonstrate their capacity to do the required work. We typically provide anywhere from $1 to $50,000 for a period of six months or less for individuals or groups carrying out relevant rapid response activities, although applications in excess of this sum can be considered. Relevant activities might include:

- Establishing new Internet connections (such as VPNs) when existing connections have been cut off or have been restricted;
- Providing personal digital protection for online journalists, human rights defenders, NGOs, activists and bloggers;
- Rapid development of tools or translations needed to respond adequately to emergencies;
- Developing decentralized, mobile internet applications that can link computers as an independent network (mesh or delay-tolerant networks);
- Emergency patches
- Any appropriate response to digital emergencies not listed above

---

Review process

Criteria

- **Quality of project idea:** When applying for direct funding, applications should exhibit originality, substance, precision, and relevance to the mission of promoting freedoms of expression, assembly, and association online.
- **Ability to achieve objectives**: A relevant work plan should demonstrate substantive undertakings and logistical capacity of the organization. The work plan should adhere to the program overview and guidelines described above. Objectives should be ambitious, yet specific, measurable, achievable, relevant and time-bound. For complete scopes of work, applicants will have to provide a monthly timeline of project activities.
- **Multiplier effect/sustainability**: Proposed programs should address how the expected results will contribute to improving Internet freedom goals.
- **Applicant record and capacity**: OTF will consider the past performance of prior recipients and the demonstrated potential of new applicants.

Submissions are viewable by the OTF team for evaluation and acceptance. To this end, all Rapid Response requests are reviewed and approved by the OTF team to assess the project's necessity, appropriateness, risk, legality, and contractual structure. Though we cannot guarantee absolute secrecy of information disclosed, we seek to avoid disclosure of

sensitive information beyond the OTF team. We strive to assess and approve Rapid Response applications as quickly as possible, *and make every effort to make a decision within five days.*

Award information

Any organization or person within OTF's remit who requires urgent assistance related to a digital emergency can apply to the Rapid Response Fund through the request form found on our website.

Recognizing that digital emergencies and response to those emergencies are unique to each situation, we individually tailor monitoring and evaluation (M&E) of these efforts. M&E can include a periodic report on the successes and/or shortfalls of the support, a report back upon completion of support, or some other appropriate method of communication.

Application requirements, submission, and deadlines

OTF accepts applications on a rolling basis.

Before completing a submission, we strongly encourage you to review our Terms of Service. If you have any questions at all, please email us at hello@opentech.fund.

You can stay up to date on all other OTF submission deadlines and open submissions windows for other potential funders by joining the OTF-announce mailing list. To subscribe to the mailing list, please submit your email address to this page.

Eligibility

Do not let the below scare you away. Consider these as a starting point for discussion, **and always apply**. If you have any concerns, please contact us directly at hello@opentech.fund. That said, individuals should meet one of the following criteria in order to be eligible for funding:

- Individuals of all ages irrespective of nationality, creed or sex;

- Individuals who demonstrate skill and ability to conduct rapid response work;
- Individuals who have intimate knowledge of the communities they are working with, and the digital threats they experience.

We are not able to support applicants within countries that the United States has trade restrictions or export sanctions as determined by the U.S. Office of Foreign Assets Control (OFAC).

All payments will be made in U.S. dollars (USD) and will comply with local laws, regulations and ethics rules. Each applicant is responsible for the tax consequences of any support they receive, as determined by the laws of their country.

It is each individual and organization's sole responsibility to comply with any policies any pre-existing employer, etc. may have that would affect your eligibility to receive support from OTF.