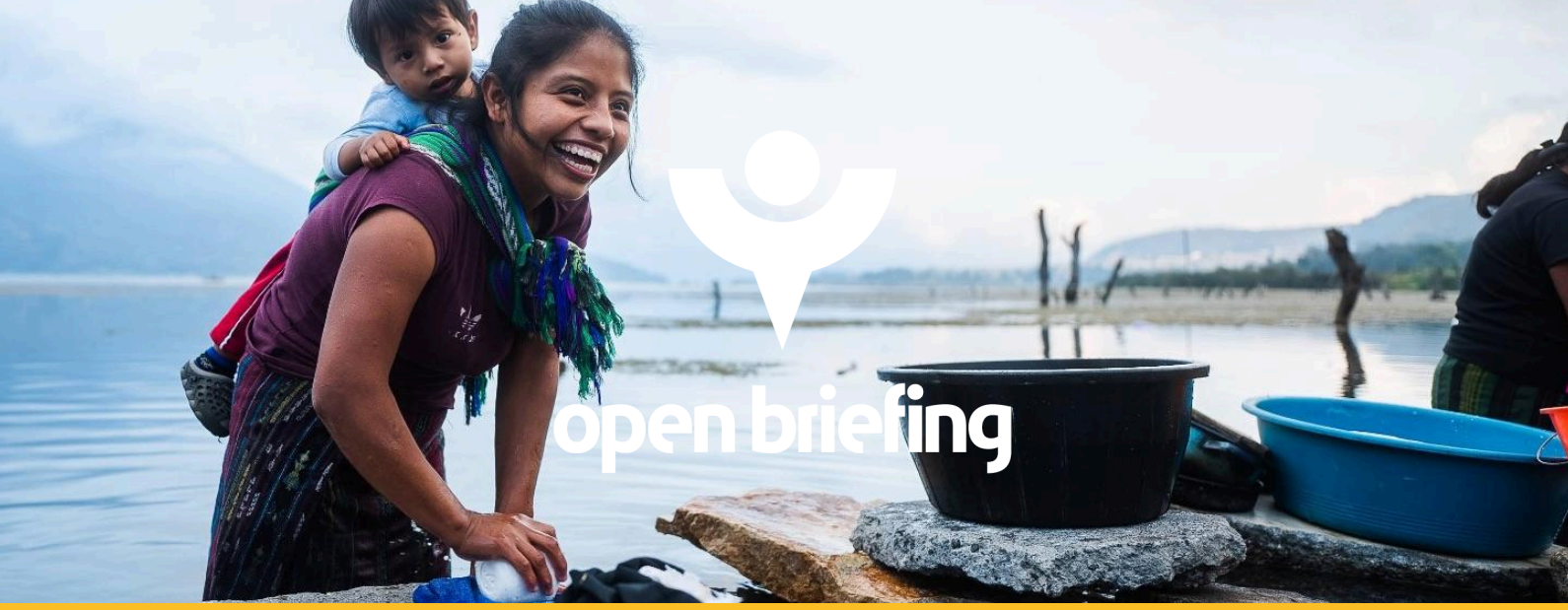

INFORMATION SECURITY CONSULTANTS

Background

A just and equitable world where communities and ecosystems can thrive is possible. But social injustice, democratic backsliding, and the climate crisis threaten us all. The courageous people and communities daring to speak out face attacks and reprisals from powerful vested interests. Many pay the ultimate price.

Open Briefing is a vital part of the response. **We build resistance and resilience among the people and communities challenging power.** And we are answering more calls for assistance across more countries than ever before. Last year, our international team provided nearly 6,000 hours of direct support to activists and advocates under threat of physical, digital, and psychological harm across 68 countries.

Alongside this local support, we provide **consultancy and advisory to help nonprofits and foundations supporting and resourcing grassroots change to take the *right* risks.** We ensure that these international partners are equipped and empowered by enhancing their security risk management, information security and data protection, and staff care and wellbeing.

Our team protects many high-profile activists and well-known organisations. But much of our work is behind the scenes, with ordinary people and communities who are targeted for challenging power. For 12 years, we have worked together towards a better future. And we are just getting started. We are expanding our diverse, inspired, and purpose-driven team; will you join us as one of our new information security consultants?

Role description

You will play a key role in helping to secure the most-valuable and -sensitive information of organisations and activists fighting for a just and equitable world. Your primary responsibilities will include:

1. Provide information security mentoring and remote accompaniment to human rights defenders and other activists and advocates facing attacks and reprisals.
2. Provide information security consultancy and advisory to nonprofit and foundation clients who are supporting and resourcing grassroots change.

You can learn more about our approach in our series of blog posts on information security.

Person specification

Essential

- You will have a proven track record of working in **information security** or **data protection** roles.
- You will have a proven track record of working with nonprofits, foundations, and/or activists.
- You will have expertise and experience that goes beyond digital security to include why and how threat actors actually seek to:
    - compromise, damage or destroy valuable or sensitive information assets; and
    - breach anonymity using public and private information.
- You will be comfortable working across the range of technologies, policies, and practices required to keep information assets safe.
- You will usually be available to take on new assignments by agreement within 2-3 working days.
- You will be sensitive to the progressive and rights-based missions and diverse profiles of our clients and other stakeholders.
- You will have excellent written and spoken English.

Desirable

- You may have a proven track record of working with or providing professional advice to senior leadership.
- You may understand data protection regimes, such as GDPR, HIPAA, and COPA.
- You may have excellent written and spoken French, Spanish, Portuguese, or Arabic.

Terms and remuneration

We are a remote-first organisation, and this is a **home-working role.** We are looking for someone who wants to become part of our close-knit team and develop a long-term working relationship with us and our clients. You will be properly onboarded and continually supported by empowering managers and highly-experienced colleagues. Your line manager will be our director of digital and information security, Dr Richard Tynan.

We welcome applications from established consultants with a range of backgrounds, experiences, and profiles, and from anywhere in the world. The hours can vary from month to month, depending on demand and your availability, and the role may require occasional remote meetings outside of normal office hours depending on your location. **Please note that this role is not suitable for those in full-time employment or currently searching for full-time employment.**

You will receive **£52.50 per hour** (equivalent to £420 a day), ongoing mentoring and training, and a package of wellbeing and mental health support, including an Employee Assistance Programme.

You will need to have or obtain your own professional indemnity insurance, including cover for work in the United States.

Diversity, equity, and inclusion

Open Briefing values diversity. We are committed to being equitable and inclusive, and to being a place where all can be their authentic selves. We therefore encourage applications from all who may meet the person specification and particularly from candidates who are from historically-marginalised groups that are underrecognised in our team. **This currently includes Black, Indigenous, and People of Colour; people from countries in the global majority; and women and/or non-binary people.** Please read our diversity, equity, and inclusion policy for more information.

Open Briefing is a Disability Confident Employer. We welcome applications from neurodivergent candidates and those who may need reasonable adjustments during the recruitment process and any subsequent employment. **Please let us know in your cover letter how we can be the recruiter and employer that you need us to be.**

We follow the gender pay gap reporting guidance from the UK government. This reveals that women currently have higher mean (average) pay than men in our organisation. We have also checked the text of this advert using the Gender Decoder tool.

How to apply

To apply, please email your CV to our office manager, Lauren Smith, at lauren.smith@openbriefing.org. Please also include a cover letter of no more than two pages setting out:

1. What excites you about Open Briefing and the role of information security consultant.
2. How you meet the advertised person specification.
3. A time when you had to move a client or colleague away from focussing on digital security solutions in order to properly manage the risks to their information. (You might set out how you engaged with the client or colleague, what the information-first solution included, and what the biggest challenges in implementing the solution were.)

We will conduct interviews on a rolling basis until we recruit suitable candidates. If you are interested in this role, **please submit your application as early as possible.**