International Foundation for Electoral Systems

IFES Tech4Democracy

Terms of Reference

I. Background

Not since the end of the Cold War have democracy and electoral integrity been so threatened around the world. In the effort to promote democracy and free and fair elections, technology and social media have often been used to achieve positive outcomes, from securing the ballot to updating voter registries to sharing information on candidates' platforms. However, malign actors are increasingly misusing technology, including social media, to undermine democratic and electoral systems with far-reaching impacts on individuals and societies. The mission of the International Foundation for Electoral Systems (IFES) is to work with partners to build resilient democracies that deliver for all, and thus our mission is directly threatened by the increasing misuse of technology to undermine democracy and elections. Consequently, one of our four strategic outcomes is for technology, information, and data to positively serve democracy and elections. To advance this strategic outcome, IFES must be proactive, agile, and creative, partnering with governments, civil society, foundations, and the technology sector to develop effective ways to counter the threats to democracy and elections posed by technology. However, IFES is primarily a project-funded organization with no core budget, and hence is significantly constrained in investing in the research, development, and innovation required to counter these identified threats. Thus, IFES has established Tech4Democracy (T4D), a fund that strengthens our ability to innovate and provide solutions for our partners in this critically important field.

II. Purpose

Core Objectives of Tech4Democracy

- Conducting research and analysis on threats to democracy and elections from technology
- Developing and deploying tools to counter the most pressing vulnerabilities
- Developing and deploying tools and mechanisms to support the positive use of technology in elections

The purpose of T4D is to promote the use of information and technology, including social media platforms, in ways that contribute positively to democracy and elections, and to mitigate against the use of information and technology in ways that harm democracy and elections. T4D provides resources to support IFES data collection and analysis on emerging threats to democracy and elections from technology, as well as the development, testing, and deployment of tools and responses to counter the most pressing vulnerabilities, in collaboration with technology firms and other partners where appropriate. T4D accelerates IFES' deployment of new and innovative programmatic tools designed to promote the appropriate use of technology and information in elections and in support of democracy.

III. Statement of Need

Research and targeted analysis are needed to properly understand emerging challenges and design tools and technical guidance with global applicability – particularly with respect to malign state and nonstate actors manipulating technology platforms to undermine public trust in democratic processes and institutions. These actors are acting aggressively and developing new tools and capabilities that heighten the risks to democratic societies. It is critical and urgent that good-faith actors – including governments, civil society, and technology companies – are proactive and collaborative in designing ways to effectively counter these constantly growing threats. IFES is committed to doing its part, including through research and development and the deployment of new and innovative tools and programmatic approaches in partnership with others.

As a worldwide leader in the democracy and elections space, IFES must proactively assist our partners – primarily governments, electoral management bodies (EMBs), and civil society – favorably manage technology's steadily increasing impact on democracy and elections. Research, analysis, and tools development supported by T4D focus on strengthening deterrence detection and mitigation mechanisms targeting a range of malign actors, the tactics they use and the diverse and often overlapping objectives driving them – such as the manipulation of election outcomes, achieving specific foreign policy goals, undermining confidence in democratic systems, and financial gain.

Two initial areas of focus are:

- **Cybersecurity Incursions in Election Systems** Many EMBs lack the capacity to deal with vulnerabilities in their technology and data management systems and to apply best practices for securing data while also maintaining a transparent electoral environment. As IFES noted in a 2018 publication on cybersecurity in elections, "Cybersecurity should be considered and implemented at the inception phase of building or upgrading any technology-based election system, as a key component of digitizing specific elements of election administration. At the same time, international good practice around cybersecurity and open data requires EMBs to act transparently and to ensure election results are verifiable and can ultimately be accepted by the electorate. Therefore, it is important to protect both cybersecurity and transparency in the electoral context – a challenge that is particularly unique to EMBs."[1]

[1] For example, other state actors such as from the defense sector, or institutions such as banks or insurance agencies, can focus primarily on cybersecurity without the same transparency concerns.

- **Technology-Fueled or Amplified Disinformation Campaigns** Malign actors are increasingly misusing technology to conduct mis- and disinformation campaigns – rife with widely shared, inaccurate, and polarizing information – in countries around the world. These campaigns seek to amplify existing and often deep-seated sources of tension in society in ways that increase social division, undermine public trust in democratic institutions, and increase the possibility of electoral violence and political instability. New and emerging technologies and tactics, including artificial intelligence, deep fakes, content or click farms, and bots and botnets, among others, take advantage of numerous apertures – both automated and human-curated – for rapidly disseminating such content as part of calculated influence campaigns.

Given the rapidly changing technology environment, and the rapidity with which bad-faith actors are learning, these categories are illustrative and likely to evolve.

In addition to improving the ability to counter existing threats and anticipating new ones, T4D supports initiatives that consider what the changing technology context may mean for democracy and governance programming: e.g., where legal changes are needed to accommodate the appropriate use of technology; an evolving understanding of how transparency and inclusion can be ensured by EMBs; the institutional structure and organizational culture needed for EMB success; or effective voter and civic education approaches that respond to the evolving ways in which individuals consume information and assess its reliability, accuracy, and neutrality. Through its support of this research and analysis, T4D establishes a foundation for the development of new tools and mechanisms for appropriate deployment of technologies.

IV. Funding

Sources of Funds T4D is resourced via two main funding avenues: a) a 10 percent levy on the total funded value of any agreement between IFES and a technology company; and b) donations from individuals, foundations, private sector corporations, or other sources.

Use of Funds T4D is intended to support IFES' efforts to promote the responsible use of technology and information in ways that strengthen democracy and electoral integrity, and to proactively address emerging threats to democracy and electoral integrity from technology. The fund is designed to be flexible and to promote innovation in ideas and agility in action. Given the potentially wide range and scope of activities, IFES has established periodic strategic review processes to ensure that activities are targeted, appropriate, and bolstering IFES' research, analytical, and programmatic capabilities.

Private sector resource contributions to this fund are subject to the provisions of the IFES Terms of Engagement with Technology Actors, which governs IFES collaboration with technology actors and ensures that IFES maintains its ability to advocate for its mission effectively and independently.

V. Background and IFES Expertise

IFES undertakes a variety of applied research initiatives to help address emerging challenges in democracy support, including those with an emphasis on the threats to elections from technology. For example, drawing on interviews with election commissioners across the globe, we have developed and tested an executive curriculum for electoral leaders to bolster their independence during a crisis – as an election can fail if those managing it are not equipped to deal with new challenges or threats. To fortify EMBs against emerging cyber threats, we have developed a Holistic Exposure and Adaptation Testing (HEAT) process to identify and mitigate technology vulnerabilities that can be exploited. We are also currently undertaking an extensive research effort to identify the most effective program and policy responses to democratic transitions, based on the past 20 years of programming. All of IFES' research is designed to produce or strengthen programmatic tools, enabling IFES to work together with partners to achieve meaningful impact in pursuit of our mission to build resilient democracies that deliver for all.