GNI Statement on the Release of Digital Services Act Risk and Audit Reports

The Global Network Initiative (GNI) welcomes the release of the first risk assessment, risk mitigation, and independent audits reports published pursuant to Article 42(4) of the European Union's Digital Services Act (DSA). This milestone marks an important step toward enhancing transparency and accountability for large digital services, objectives that align with GNI's long-standing commitment to promoting responsible business practices.

These reports should offer a valuable opportunity to understand how Very Large Online Platforms and Search Engines (VLOPSEs) identify and mitigate "systemic risks" related to their services. We hope they will allow civil society organizations, regulators, policymakers, other industry stakeholders, and users to identify opportunities for shared reflection and further engagement to enhance rights protections in Europe and globally.

Over a decade-and-a-half ago, GNI pioneered a unique multistakeholder assessment process that facilitates the evaluation by independent, GNI-accredited assessors and GNI members, of company efforts to implement systems and processes to respect users' rights in line with the GNI Principles for Freedom of Expression and Privacy and Implementation Guidelines. Since then, GNI member companies have voluntarily participated in these assessments, sharing non-public information and receiving feedback on their efforts to address risks to freedom of expression and privacy. Through four cycles of these multistakeholder "assessments," as well as many additional resources, learning sessions, and events, GNI has developed and shared valuable insights into the challenges and opportunities faced by a wide range of companies operating across the tech sector. This has included identifying good practices around stakeholder engagement, human rights due diligence risk assessment and mitigation, and transparency, all of which we believe are in line with the expectations set out in the DSA. Given the number of GNI companies whose services have been designated as VLOPSEs, we have also worked to adapt our assessment process to complement mandatory due diligence regulations including, but not limited to, the DSA.

GNI regularly scrutinizes government efforts to regulate the tech sector, calling out potential intended *and* unintended consequences that would infringe on freedom of expression or privacy. We engaged on the DSA from its earliest consultations and consistently expressed concern about the potential for overreach, while articulating support for its focus on the development of systems for identifying and mitigating human rights risks, in line with the United Nations Guiding Principles on Business and Human Rights (UNGPs) and the OECD Guidelines on Multinational Enterprises (OECD Guidelines). Building on this experience, GNI has recently worked to foster information sharing and dialogue across stakeholders around DSA compliance. GNI believes companies should adopt a global approach on risk assessment and mitigation, and

uphold the rights of all users around the world. Engaging and sharing information among stakeholders, including from underrepresented communities, can help improve regulatory design and implementation, including corporate compliance and government enforcement, while safeguarding fundamental rights.

In the coming months, we will continue to engage with the European Commission, EU Digital Service Coordinators, authorities in other regions, and a wide range of stakeholders to enable further learning and improvement around tech company risk assessments and mitigations, and to ensure these regulatory processes lead to meaningful accountability and protection of fundamental rights. GNI will also continue adapting its assessment process in future cycles to take into account the DSA and other mandatory due diligence regulations, where appropriate, in order to enhance accountability, improve the effectiveness and efficiency of both types of assessments, and contribute to the identification of best practices.