G7 Digital & Tech Ministerial Meeting on Frontier AI Model Security – Chair's Statement

Digital & Tech Ministers and representatives of the G7 and the OECD gathered in a ministerial meeting organized by French Minister delegate for AI and digital affairs, Ms. Anne Le Hénanff, on October 20th, 2026, to discuss avenues of cooperation between G7 partners on the issue of Frontier AI Model Security.

The meeting highlighted that rapid advancement and large-scale deployment of AI across critical domains can bring transformative opportunities, such as productivity gains, improvements to public services, and advances in, notably, science and healthcare. However, the discussion pointed out that Frontier AI models and systems ("Frontier AI models") can pose certain risks arising from cybersecurity or unintended behavior which could lead to loss of control scenarios, among other adverse impacts. They may also be misused by malicious actors, including in the areas of malicious cyber activities and the development of chemical, biological, and radiological capabilities. The French G7 Presidency recognized that Frontier AI models transcend national borders in their development, deployment and impact, and that their opportunities and risks are therefore inherently global.

In this context, following discussions among G7 leaders at the Évian Summit, and building on the *Hiroshima AI Process* and the *G7 Digital and Technology Ministerial Declaration* of 29 May 2026, G7 Digital & Tech Ministers and representatives explored ways to reinforce cooperation on Frontier AI model security matters.

Considering that the discussions highlighted a number of converging approaches within G7 members' respective jurisdictions, they discussed a range of appropriate measures that could be taken by Frontier AI model providers throughout their development, including prior to and throughout their deployment and placement on the market, to identify, evaluate, and mitigate risks across the lifecycle.

The discussions also underlined the need for a coordinated, converging approach between G7 members on the understanding, identification and information sharing of risks and incidents related to frontier models, and the unique role the G7 can play as a relevant coordination platform between like-minded partners on the issue of Frontier AI model security.

While discussing the relevance of such approaches to G7 coordination on this matter, it was deemed useful to draw on the work of G7 members' national bodies and agencies with competence in Frontier AI model security, or other relevant international organizations or initiatives, in voluntary association with Frontier AI model developers and independent experts. Such organizations and initiatives could include among others the *International Network for Advanced AI Measurement, Evaluation and Science*, international standardization bodies, the OECD *Working Party on AI Governance*, and the *Hiroshima AI Process Reporting Framework*.

The discussions allowed G7 members to consider several potential avenues to reinforce G7 coordination based on existing G7 channels[1], including the option of a dedicated High-Level Group with a view to facilitating coordination among the relevant G7 tracks, including in the event of a serious, fast-moving, cross-cutting Frontier AI model-related development.

1 The Digital and Tech Working Group; the Cybersecurity Working Group (which brings together national cybersecurity agencies and centers); the Cyber Expert Group (which brings together the cyber experts of national financial supervisors, including finance ministries and central banks, and is attached, under the French G7 Presidency, to the Finance track); and the Ise-Shima Cyber Group (attached, under the French G7 Presidency, to the Foreign Affairs track).