Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware

We, the governments of Australia, Canada, Costa Rica, Denmark, Finland, France, Germany, Ireland, Japan, New Zealand, Norway, Poland, Republic of Korea, Sweden, Switzerland, the United Kingdom, and the United States, recognize the threat posed by the misuse of commercial spyware and the need for strict domestic and international controls on the proliferation and use of such technology.

Commercial spyware has been misused across the world by authoritarian regimes and in democracies. Too often, such powerful and invasive tools have been used to target and intimidate perceived opponents and facilitate efforts to curb dissent; limit freedoms of expression, peaceful assembly, or association; enable human rights violations and abuses or suppression of civil liberties; or track or target individuals without proper legal authorization, safeguards, or oversight. The misuse of these tools presents significant and growing risks to our national security, including to the safety and security of our government personnel, information, and information systems.

We therefore share a fundamental national security and foreign policy interest in countering and preventing the proliferation of commercial spyware that has been or risks being misused for such purposes, in light of our core interests in protecting individuals and organizations at risk around the world; defending activists, dissidents, and journalists against threats to their freedom and dignity; promoting respect for human rights; and upholding democratic principles and the rule of law. We are committed, where applicable and subject to national legal frameworks, to implementing the Guiding Principles on Government Use of Surveillance Technologies and the Code of Conduct developed within the Export Controls and Human Rights Initiative.

To advance these interests, we are partnering to counter the misuse of commercial spyware and commit to:

- working within our respective systems to establish robust guardrails and procedures to ensure that any commercial spyware use by our governments is consistent with respect for universal human rights, the rule of law, and civil rights and civil liberties;
- preventing the export of software, technology, and equipment to end-users who are likely to use them for malicious cyber activity, including unauthorized intrusion into information

systems, in accordance with our respective legal, regulatory, and policy approaches and appropriate existing export control regimes;

- robust information sharing on commercial spyware proliferation and misuse, including to better identify and track these tools;
- working closely with industry partners and civil society groups to inform our approach, help raise awareness, and set appropriate standards, while also continuing to support innovation; and
- engaging additional partner governments around the world, as well as other appropriate stakeholders, to better align our policies and export control authorities to mitigate collectively the misuse of commercial spyware and drive reform in this industry, including by encouraging industry and investment firms to follow the United Nations Guiding Principles on Business and Human Rights.

Our efforts will allow us to work collectively for the first time as we develop and implement policies to discourage the misuse of commercial spyware and encourage the development and implementation of responsible use principles that are consistent with respect for universal human rights, the rule of law, and civil rights and civil liberties.