Dear Chair, Honorable delegates to the OEWG

The Forum of Incident Response and Security Teams (FIRST), was established more than 30 years ago and brings together over 600 incident response and security teams from nearly 100 countries. FIRST members are national Computer Security Incident Response Teams (national CSIRTs), CSIRTs from the private sector and academia as well as Product Security Incident Response Teams (PSIRTs). FIRST champions capacity building and knowledge exchange, and produces much needed cybersecurity standards such as CVSS and TLP.

Thank you for allowing us to contribute towards this important discussion. FIRST welcomes the continuation of the OEWG, endorsing the previous work by the UN GGE and OEWG.

FIRST has always been concerned about state sponsored operations creating large collateral damage to the Internet infrastructure and Internet-enabled services, and to Internet users. Last year, incident responders spent countless hours cleaning up after two large espionage operations. Evidence is mounting that some intelligence services collaborate with the very criminal gangs which attack critical infrastructures and health organizations. This is not acceptable.

At the same time, comprehensive sanctions, especially at the time of armed conflicts, force FIRST to exclude teams from involved countries. The 2015 UNGGE norms recommend that states must not attack incident response teams and that CSIRTs must not participate in offensive operations. The 2021 UNGGE consensus report underscores the importance of *avoiding the politicization of CERTs/CSIRTs and respecting the independent character of their functions*. Following this logic, Incident response teams (CSIRTs and PSIRTs) should be exempt from such sanctions. FIRST brings together incident response teams and helps them build capacity, network, share knowledge, and most importantly build trust to work together and cooperate even during a crisis.

To summarize, FIRST encourages this group to works towards ensuring that:

- Incident responders can continue to collaborate globally, especially in the time of a crisis
- The good of all internet users and the global Internet safety and security must be taken into account
- An open and inclusive multi-stakeholder approach is essential for successful incident response and security efforts.

Thank you very much