<u>Pursuant to the UN Office for Disarmament Affairs request to Member States to share their views on the capacities required to participate in the Points of Contact directory, including views on capacity-building experiences drawn from participating in other directories.</u>

National Cyber Security Center - Jordan has provided the following views on the capacities required including drawn from participating in other directories:

1. Participants in the POC directory should possess technical expertise in cybersecurity and related fields. This includes knowledge of cyber threats, incident response procedures, and relevant technologies.
2. Strong communication skills are crucial for engaging with other participants, sharing information, and coordinating response efforts. Clear and concise communication helps facilitate collaboration and ensure that critical information is effectively conveyed to relevant stakeholders.
3. Participants should be open to sharing information, listening to others states perspectives, and resolving conflicts constructively to achieve common goals.
4. Participants should have the ability to analyze complex cyber threats, identify trends, and develop effective mitigation strategies is essential for participating in the POC directory. Participants should be able to assess the severity and impact of incidents, prioritize response actions, and adapt their approach based on evolving circumstances.
5. Participants must adhere to ethical principles and respect confidentiality when sharing sensitive information within the directory. Upholding ethical standards helps maintain trust and credibility among participants and ensures the integrity of collaborative efforts.

Insights drawn from participating in other directories, such as those focused on threat intelligence sharing or cybersecurity incident response, can provide valuable lessons for building capacity within the POC directory. Some key experiences include:

1. Training and Knowledge Sharing: We are participating in other directories (Local and International CERT) which give us opportunities for training, workshops, and knowledge-sharing sessions. These experiences can enhance participants' technical skills, deepen their understanding of cyber threats, and strengthen their ability to collaborate effectively within the POC directory.
2. Establishing Trusted Relationships: Building trust and fostering relationships with other participants is critical for successful collaboration in any directory.
Experiences gained from participating in other directories can provide insights into effective relationship-building strategies and best practices for establishing trust among participants.
3. Navigating Legal and Policy Considerations: Many directories operate within a legal and regulatory framework that governs the sharing of sensitive information.
Experiences from participating in other directories can offer valuable insights into navigating legal and policy considerations, ensuring compliance with relevant laws and regulations, and addressing data privacy and security concerns.

All in all, the capacity-building lessons learned from other directories can offer valuable lessons and best practices for effective Points of Contact involvement. Participants can use their technical knowledge, communication and collaboration skills, and experience gained from previous experiences to strengthen their ability to work together to tackle cyber threats