Implementation of Cyber and International Data Transfer Pre-Qualification Criteria in National Wind Energy Auctions

The recent Wind Power Package and the design guidance for non-price criteria in renewable energy auctions advises that Member States incorporate pre-qualification standards related to cybersecurity and international data transfer in their wind energy auctions, aligning with EU regulations and international commitments. The Net Zero Industry Act will mandate these criteria for Member States when organizing auctions for technologies deemed strategic for achieving net-zero emissions.

Currently, various EU laws are being developed or enforced to tackle cybersecurity and data security exchange within the energy sector. These laws include the Network and Information Security Directive (NIS 1 and NIS 2), the EU Cyber Resilience Act (EU CRA), the EU Data Act, and the Network Code for Cyber Security in cross border electricity flows (NCCs). The European Commission will need to issue guidance on how these pre-qualification standards should be practically implemented at the national level, considering the comprehensive existing regulatory landscape. This guidance should leverage established channels created through EU legislation, such as NIS2 and the Cyber Entity Resilience Directive, ensuring consistency and coherence across all regulatory measures.

1. **Risk Assessment for Cybersecurity and Data Security**

Proposed Legal Text: "The bidding entity must demonstrate a comprehensive approach to managing cybersecurity and data security risks associated with the operation of the entire fleet of their assets. This approach must encompass the equipment including software and hardware components, and comply with recognized international standards such as ISO, IEEE, and IEC or their equivalents."

Implementation:

- **International Standard Compliance:** National Authorities should mandate adherence to international standards.

- **Documentation and Verification:** Bidders must document that their risk assessment process have balanced potential national and economical lose for the expected lifetime of the asset in a structure manner. Regulatory bodies should implement a verification process, before the asset get connected to the grid, potentially involving third-party audits.

- **Continuous Improvement:** National Authorities should require bidders to update their risk management practises regularly in response to evolving threats and technological advancements, enforced through periodic reviews and updates.

- **Diversification of Components:** Strategies should differentiate between active components (e.g., cybersecurity components) and passive components (e.g., cables, connectors, structural elements), ensuring thorough risk management.

2. **Requirements for Prioritizing Technology Suppliers Based on Data Handling Locations within EU Customs Union and GPA Signatory Countries**

Proposed Legal Text: "Bidders must prioritize technology suppliers that, following a thorough risk assessment, commit to storing, analysing, and sharing data with significant impact only in countries within the EU Customs Union or signatories of the Government Procurement Agreement (GPA) that apply standards equivalent to the General Data Protection Regulation (GDPR), considering national security aspects as permitted by Treaty of functioning of European Union (TFEU) Article 346."

Implementation:

- **Supplier Vetting:** Bidders must provide evidence of thorough due diligence in selecting technology suppliers, including contractual clauses ensuring compliance with GDPR-equivalent standards. Additionally, a risk assessment considering national security aspects must be included.

- **Data Residency Requirements:** National Authorities should mandate data residency requirements, considering national security aspects, before the asset is integrated into the grid to ensure that data with significant impact is processed and stored within jurisdictions adhering to stringent data protection regulations. This may involve collaborative efforts with other EU member states or GPA signatories to optimize the use of existing secure data centres.

- **Monitoring and Enforcement:** Regulatory bodies should monitor compliance through regular audits and impose penalties for non-compliance, involving cross-border cooperation with data protection authorities. Monitoring should also include assessments of national security implications.

3. **Regular Assessment of Cybersecurity and Data Security Risks**

Proposed Legal Text: "Bidders must commit to regularly assessing cybersecurity and data security risks associated with the operation of the equipment installed as part of their successful participation in the auction."

Implementation:

- **Periodic Risk Assessments:** National Authorities should mandate that qualified professionals conduct periodic risk assessments, such as annually, covering all aspects of the operation, including hardware, software, and data handling practices.

- **Reporting and Accountability:** Bidders are required to submit comprehensive risk assessment reports to a designated national authority, detailing identified risks, mitigation measures, and any incidents of non-compliance.

- **Incident Response Plans:** National Authorities should mandate that bidders develop and maintain incident response plans to ensure rapid and effective responses to cybersecurity and data security breaches, with regular tests and updates.

- **Diversification of Components:** Risk assessments must address both active and passive components, ensuring a comprehensive evaluation and effective mitigation strategies for all elements involved.