DIGITALISATION AND CYBER SECURITY EXPERT

Technical Assistance package for the Sustainable Energy Support Programme in Tajikistan

Terms of Reference for Short Term Expert	
Expert position	**Digitalisation and Cyber Security Expert**
Expert Category	Senior Non-Key Expert
Mission start-end date	01.03.2024 – 13.11.2027
Minimum requirements	*Skills and qualifications:* ▪ A University degree in Cybersecurity, Information Technology, Electrical Engineering, or a related field. *General experience:* ▪ Minimum of 12 years of professional experience in the field of Information Technology ▪ Experience in digitalisation and cybersecurity projects within the energy sector. ▪ Knowledge of the latest electricity sector-related cybersecurity standards and regulations. ▪ Fluency in English; knowledge of Tajik and/or Russian would be a plus. *Specific experience:* ▪ Proficiency in cybersecurity risk assessment and management. ▪ Familiarity with SCADA and energy management systems. ▪ Excellent communication and interpersonal skills. ▪ Ability to work collaboratively in a multicultural environment.
Duration/working days	Up to 410 working days
Task(s) assigned	**Key Responsibilities**: ▪ Support to the MoEWR lead innovation and digital transformation of electricity systems, adhering to the best industry standards, and installing a robust, resilient, and secure structures for safeguarding electricity systems against potential malicious cyber threats. **Digitalization Strategy**: ▪ Support MoEWR develop and implement a comprehensive digitalization strategy for the electricity sector in Tajikistan, aligning it with European Union and international best practices. **Cybersecurity Framework**: ▪ Assist MoEWR establish and maintain a robust cybersecurity framework, tailored to national and regional requirements of electricity industry, considering industry's best, and most up to date standards and guidelines (i.e. ISO 27001, NIST Cybersecurity Framework, NERC CIP, IEC 62443 etc.), and support ensuring compliance with selected/adopted standards and regulations. **Risk Assessment**: ▪ Conduct regular risk assessments to identify potential vulnerabilities and threats specific to the electricity sector's digital infrastructure and critical assets. **Security Architecture**: ▪ Guide MoEWR design and oversee the implementation of secure architecture for energy sector digitalization initiatives, including advanced control systems, SCADA, and IoT devices, and support placing measures safeguarding resilience against cyber threats. **Incident Response**: ▪ Support development and maintenance of a comprehensive incident response plan and related emergency response mechanisms, ensuring efficient and coordinated actions in the event of cyber incidents. Assist MoEWR on

	continually improving response capabilities to mitigate cyberattacks and ensuring the rapid recovery of critical systems. **Compliance and Standards**: ▪ Stay up to date with evolving cybersecurity regulations, standards, and best practices specific to the electricity sector, and ensure compliance/adherence to them across all sub sectors and initiatives. **Collaboration**: ▪ Foster collaboration with relevant national or reginal government agencies, energy utilities, regulatory structures, and international organizations to promote information sharing and enhance the nation's cybersecurity posture and regional interlinkages. **Capacity Building**: ▪ Provide training and mentorship to internal MoEWR and utilities' personnel for maintaining and improving cybersecurity practices. ▪ Support training and capacity-building programs for relevant ministry and utilities personnel, external partners and stakeholders to enhance cybersecurity awareness and skills. **Security Awareness**: ▪ Assist MoEWR develop and support implementation of cybersecurity awareness campaigns for all stakeholders within the electricity sector, emphasising the importance of vigilance and adherence to security protocols. **Security Audits**: ▪ Conduct regular security audits and penetration testing to assess the effectiveness of cybersecurity measures and identify areas for improvement. **Partnerships**: ▪ Collaborate with international organizations, cybersecurity experts, and relevant stakeholders to share knowledge and stay informed about emerging threats and solutions. **Research and Innovation**: ▪ Stay at the forefront of technological advancements and emerging threats in the electricity sector to continuously enhance security measures and adopt innovative solutions. **Budget Management**: ▪ Manage financial resources effectively to support cybersecurity initiatives, including procurement of necessary tools, technologies, and services. Reporting: **Reporting**: ▪ Prepare comprehensive reports on the status of digitalization and cybersecurity initiatives, including incident reports, compliance status, and recommendations for improvements.
Output(s)	Inception, mission and progress reporting, etc. as requested to include close cooperation with other development partners and development of the cyber security RoadMap, proposed by the World Bank