LCNF Full Submission

Supplementary Answer Form

DNO Name:	Electricity North West Limited	**Question Number:**	ENWL027
Question Date:	17 Sept 2010	**Answer Date:**	21 Sept 2010
Question Topic:		Box 13	

Original Question No:		**Original Answer Date:**	
Original Question:			
Original Answer:			

Question:	Please confirm why the specific "Cyber Security Solution" is critical to this proposal and that this is not BAU for such applications? Is this a propertiary system

Answer:	The implementation of a cyber security solution for any project that extends the scope of the existing communications operational network beyond its existing reach is business as usual. However the potential scale of such a network presents challenges not previously encountered. The following identifies some of the challenges to show that our approach to cyber security will not be a business as usual approach: • The communications operational network serves major substations such as Grid Supply Points, Bulk Supply Points and Primary Substations, some 450 end points in total. These substations are large in size and have maximum physical security. Communications to these substations has traditionally been serial using protocols that are not generally in the public domain and difficult to break into and it is reasonably easy to firewall this scale of network against third party interference; • The move to Internet Protocol (IP) based networks presents a specific challenge in that using open protocols potentially exposes the network to third party interference using standard

	PC equipment and standard off the shelf routers and switches; • The number of endpoints in a Smart Grid increases significantly from a few hundred to potentially hundreds of thousands. These additional end points are located in distribution substations and customer premises where the physical security level is much lower than that associated with the major substations currently served; • The communications technologies for use in Smart Grids such as WiMax, DSL and Powerline Broadband based on IP protocols are relatively new and have not been deployed on a large scale in the UK; • The technologies used in securing such networks (Ruggedised Routers, Switches, Certificate Servers, Radius Servers all Dot1x capable, Dot1x being a clearly defined standard for port based authentication) are not new however the sheer potential scale of such a network in itself presents a challenge in managing both authentication of user and device level connections to the network and in managing the volume of equipment deployed; and • Historically the data being handled related to components within the distributors' netwok. Increasingly the type of data being handled will be related to specific customer nodes, and hence the aspect of customer data privacy and security needs specific consideration above business as usual.

Attachments:	None.