NATIONAL CYBER SECURITY STRATEGY 2019 - 2024 MID-TERM REVIEW

ESB Networks’ Response to Consultation

7th February 2023

1 Introduction

ESB Networks welcomes the opportunity to respond to the Department for Environment, Climate and Communication's consultation paper on 'National Cyber Security Strategy 2019 – 2024 Mid-term Review'. Given the potential damage that could be caused to national systems and infrastructure by a cyber breach, it is essential that relevant policy continues to evolve to meet this growing challenge.

ESB Networks supports the work being undertaken by the National Cyber Security Centre (NCSC) and will continue our engagement and support of its activities. To date we have embraced the vision and objectives as set out by the NCSC and have embedded them as appropriate within our own organisational structures. It is essential that ESB Networks secure our systems from the evolving risks of cyber threats and attacks in line with best practice appropriate to critical electrical infrastructures.

Given the ever-changing cybersecurity landscape and the increasingly prevalent cybersecurity threats that have both directly and indirectly affected systems, ESB Networks believe that the evolution (through the mid-term review) and implementation of this strategy is of increasing importance.

1.1 Role of ESB Networks

As DSO, DAO and TAO, ESB Networks works to meet the needs of all Irish electricity customers, providing universal affordable access to the electricity system, and delivering and managing the performance of a system of almost 155,000 km of overhead networks; 23,000 km of underground cables; 640 high voltage substations; significant amounts of connected generation, including 5.4 GW of renewable generation connected to the Distribution and Transmission systems; 2.5 million demand customers; and now several thousand "active customers" – including but not limited to domestic premises with microgeneration (a rapidly increasing number), demand side management, houses with battery storage, etc.

ESB Networks also delivers a range of services to the Republic of Ireland (RoI) Retail Electricity Market servicing over 2.5 million customers. We manage relationships with market participants and provide data in a timely and accurate fashion on a daily basis. ESB Networks supports the wider RoI market through the ring-fenced Meter Registration System Operator (MRSO) and Retail Market Design Service (RMDS) and supports the wholesale Single Electricity Market through the provision of aggregated meter data.

The infrastructure that ESB Networks operates is critical to Ireland's economy and society, and ESB Networks is committed to maintaining the security and resilience of its IT (Information Technology) and OT (Operational Technology) environments that support critical infrastructure and data by applying security-by-design and defence-in-depth principles.

ESB Networks' cybersecurity requirements are defined by the increased automation and smart grid technologies, growth in the use of electric vehicles (including smart charging technology), growth in small-scale generation (and future needs for controllability and system services), growth in the number of active customers (selling power produced by their micro-generation back to the grid) and more widespread deployment and use of smart meters (to enhance network performance and customer experience).

2 ESB Networks Response

ESB Networks is generally supportive of the Cybersecurity Strategy and the proposed additions as part of the mid-term review and for this reason we have not addressed each of the questions as outlined in the consultation paper. However, below we have outlined two areas which we believe require consideration for inclusion in the updated strategy and which have relevance to Measure 10, these are:

1. The strategy would benefit by drawing a distinction between the IT (Information Technology) and OT (Operational Technology) environments that support critical infrastructure. Typically, IT capital investments would have a 10-year lifecycle whereas OT capital investments would have a lifecycle up to 20-30 years. Due to this the approaches taken towards achieving cybersecurity of these environments can be different. Implementing this approach would allow for further development of the understanding of the differences between each environment, the approaches taken to ensure compliance with the relevant cybersecurity controls and the challenges that are faced while implementing cybersecurity improvements.

   Also, while it is important to develop a common understanding of the differentiating factors between IT and OT environments and how they are protected, it is equally important to understand how these environments interact and support each other while maintaining appropriate cybersecurity controls. Although it would be expected that the number of OES (Operator of Essential Services) that this affects would be minimal, given that those bodies manage some of the state’s most critical infrastructure, ensuring their integrity is essential.

2. It should also be considered whether the strategy could allow for the creation of a sub-group within the Government IT Security Forum, established under Measure 10 of the strategy or an independent OT Security forum, to specifically discuss cybersecurity measures within an OT environment and how they interact with IT environments. This would provide a mechanism for the NCSC to develop the recommendations referenced as part of point one above.

3 Conclusion

ESB Networks welcomes the opportunity to comment on this consultation on ‘National Cyber Security Strategy 2019-2024 Mid-term Review’ and believe that the strategy is critical to ensuring that Ireland is prepared for the constantly evolving risks to cyber security.

We have outlined in this response the basis for our observations. ESB Networks remain available to discuss the comments provided in this consultation response and look forward to engaging with DECC, NCSC and other industry stakeholders as this critical area evolves.