Making a positive difference
for energy consumers

Our Ref :Draft Guidance Counsultation-RIIO2 Cyber Guidance
Direct Dial: 020 7901 1810
Email: riio2cyber@ofgem.gov.uk

Date: 13th September 2019

Dear Operators,

RIIO is Ofgem's performance – based framework to set the price controls; through their business plans, companies put forward costs, including those associated with cyber security. RIIO stands for Revenues = Incentives + Innovation + Outputs.

Network companies are due to submit Business Plans for Transmission, Gas Distribution and the Electricity System Operator, covering the RIIO-2 period, on the 9th December 2019. Ofgem published Business Plan Guidance for RIIO-2[1], which states, under paragraph 6.96, that; "…network companies must demonstrate how companies will take appropriate and proportionate technical and organisational cyber security measures to manage risks posed to the security of the network and information systems on which their essential services depend, and to prevent and minimise the impact of incidents on these essential services.". To assist in developing Cyber Resilience plans we said we would publish guidance to support network operators in formulating these plans.

Ofgem has now developed a set of draft Cyber Resilience guidance documents, to assist in RIIO-2 Operational Technology (OT) Cyber Resilience planning, based on the National Cyber Security Centre ("NCSC") sector-agnostic Cyber Assessment Framework ("CAF"). However, it is important to note that this draft guidance is not a compliance benchmark, and that overall management of risks and associated mitigation planning are the sole responsibility of the network companies. The guidance proposed here, is presented as a minimum set for RIIO-2 network companies.

This draft documents are based on NCSC guidance, International Organizational for Standardization ("ISO") 27019, International Electrotechnical Commission ("IEC") 62443, Industrial Automation and Control Systems Security ("ISA") 99, National Institute of Standards and Technology ("NIST") 800-82, NIST 800-53 and the Health and Safety Executive - Cyber Security for Industrial Automation and Control Systems ("IACS") Edition 2 Operational Guidance 86 ("OG86").

Ofgem is seeking feedback on the draft guidelines from RIIO-2 participants by 11th October 2019. This will be considered for inclusion in a subsequent version which will also incorporate changes arising from the forthcoming NCSC CAF review. Feedback can be provided to the following address: RIIO2Cyber@ofgem.gov.uk.

If you require an extension to this deadline, please contact us explaining the reasons why.

Stuart Okin,
Head of Security, Privacy & Resilience

[1] https://www.ofgem.gov.uk/publications-and-updates/riio-2-sector-specific-methodology-decision