Whitlock, Melissa

From: [redacted]@ofgem.gov.uk>
Sent: 10 February 2025 22:51
To: Helios Renewable Energy
Subject: Interested Party Reference number: 20050047 - Helios Renewable Energy Project [OFFICIAL]
Attachments: 20250129 - Helios.pdf

The Planning Inspectorate,
I refer to correspondence received from Matthew Sheard, The Planning Inspectorate dated 09th December 2024, 15:23 following the entry submitted by Ofgem on the 4th September in relation to the Helios Renewable Energy Project against which Ofgem raised the concern: -

> "that the project may pose a risk to the security of UK energy supply if the design, construction, and operation of the project does not address the requirement for cybersecurity through the adoption of appropriate and proportionate (cyber) risk management practise. The asset may well become designated at a specified CNI rating, or the owner / operator be considered an Operator of Essential Services (OES) and this needs to be considered within the planning process. This may require consideration of design aspects to add redundancy or impact the selection of location for example. The registrant is interested to understand how these will be addressed within the process."

Please find enclosed a summary statement of the meeting held with Helios representatives on the 16th January in response to the enquiry. We are satisfied that the application has addressed the question sufficiently and has taken on board the advice provided regarding codes and standards relating to (cyber) security practices including mandatory requirements, and that this will be considered appropriately by the applicant. Therefore, currently we do not need to seek any further information from the applicant. However, we would request that the applicant engages with the cyber security team within DESNZ (contacts provided) to answer the question around project ownership.

I trust this will suffice and kindly request that you if require any further comment from Ofgem to please advise accordingly using this correspondence address.

Kind Regards,

[redacted]

[redacted]
Operational Technology Cyber Architect
Cyber Regulation
10 South Colonnade
Canary Wharf
London
E14 4PU
Tel:
www.ofgem.gov.uk

Follow us on Twitter

[]

ofgem
Making a positive difference
for energy consumers

FAO: Julie Barrow,
Infrastructure Planning Associate Director,
Stantec

By e-mail: [redacted]@stantec.com

Your Ref:	Helios Renewable Energy Project (EN010140)
Our Ref:	Cyber Resilience of Energy Infrastructure
Email:	CyberSecurityTeam@ofgem.gov.uk
Date:	29th January 2025

Regarding: **Helios Renewable Energy Project (EN010140) – Meeting with project developer (Stantec) on the 16th January 2025**

Dear Julie,

Thank you for the time provided by members of the Stantec team and Enso Energy on the 16th January 2025 during which we discussed the enquiry submitted by Ofgem against Helios Renewable Energy Project (EN010140). In which Ofgem sought understanding as to how the applicant would address aspects relating to cyber security within the project proposal[1].

I wanted to capture the salient points discussed during our meeting and confirm our view of any shared understanding that was reached.

Meeting outcome: -

We are broadly satisfied with the response provided during the meeting held with the representatives from the Helios Project and do not plan to seek any further clarification on behalf of Ofgem in relation to the enquiry raised at this time.

We have provided advice on where the project developer can find guidance relating to appropriate and proportionate cyber security practice and highlighted the wide adoptance of ISA/IEC 62443 series of standards by practitioners within the sector.

We are satisfied that the applicant is aware of the need for cyber security within the design of the project according to industry codes and standards and the intention to review the applicability of the NIS regulations to assess the need to self-nominate should the qualifying criteria be met.

Our joint CA partner (DESNZ) are still seeking further understanding as to ownership structure and control of the project which remains the only area that we wish to seek better understanding.

[1] Helios Renewable Energy Project

The Office of Gas and Electricity Markets
10 South Colonnade, Canary Wharf, London E14 4PU **Tel** 020 7901 7000 **Fax** 020 7901 7066 **www.ofgem.gov.uk**

Background to the enquiry: -

Ofgem act as joint Competent Authority ("CA") for cyber security within the Downstream Gas and Electricity ("DGE") sector, alongside the Secretary of State for Energy Security and Net Zero under the Network and Information Systems Regulations 2018[2] ("NIS Regulations"). One of our responsibilities as CA is to regulate persons designated as Operators of Essential Services ("OES") in accordance with the NIS Regulations. To support this objective we are looking beyond existing OES designations to consider new entrants and determine how we should respond as the sector progresses delivery of new energy infrastructure to support the UKs clean power[3,4] ambitions.

We are aware that as our energy systems evolve, network and information systems are playing an increasingly important role in enabling a smart and flexible energy infrastructure that meets customer requirements. As a result, infrastructure assets are becoming more dependent upon digital technologies to manage and control our energy services. Learning from previous cyber security incidents, these digital systems can be an attractive target for malicious actors, and they can also be susceptible to disruption through systems failure.

We also have observed that the magnitude, frequency and impact of network and information system security incidents is increasing. Historical events such as the 2015 attack on Ukraine's electricity network and the 2017 WannaCry ransomware attack, together with more recent events such as the US Colonial Pipeline and Redcar & Cleveland and Hackney councils ransomware attacks clearly highlight the impact that incidents can have on society. Placing a greater emphasis on the security of Network and information systems and the role they play to enable and sustain essential services.

There is therefore a need to continually improve the security of network and information systems across the UK, with a particular focus on energy delivery functions which if compromised could potentially cause significant damage to the economy, the environment, and society.

Clarity sought: -

Considering future energy projects our view is that Battery energy storage systems ("BESS") are becoming indispensable to modern power grids. These systems integrate renewable energy sources, maintain grid stability and provide backup power during emergencies. Their reliability and security are becoming essential to everyday activities and should be designed cyber secure where appropriate.

As CA for the DGE sector our interest in the Helios Renewable Energy Project is to understand the cyber security measures being implemented by the developer to design and build energy infrastructure that is cyber resilient. In accordance with recognised and generally accepted industry (security) practice and, where applicable in accordance with legal and or statutory requirements for cyber security.

Information shared with the applicant : -

While we do not recommend a specific technical standard to be followed for implementation of cyber security practice by operators. DGE members are widely adopting the ISA/IEC 62443 series of technical standards as an industry norm to secure physical energy infrastructure assets that rely on network and information systems comprising industrial automation and control systems ("IACS") or more generally those systems referred to as

[2] https://www.legislation.gov.uk/uksi/2018/506
[3] https://www.gov.uk/government/publications/clean-power-2030-action-plan
[4] https://www.neso.energy/publications/clean-power-2030

The Office of Gas and Electricity Markets
9 Millbank London SW1P 3GE **Tel** 020 7901 7000 **Fax** 020 7901 7066 **www.ofgem.gov.uk**

OT.

Beyond these standards the UK technical authority, the National Centre for Cyber Security ("NCSC") publishes a comprehensive body of cyber security knowledge. Importantly the guidance provided by the NCSC covers both information technology ("IT") and operational technology ("OT") and includes a cyber assessment framework[5] ("CAF") to support responsible persons understand good security outcomes and determine gaps in attainment against a series of practices deemed necessary to build cyber resilience. This assessment framework links to a wide range of recognised good practice and industry norms for use.

For persons qualifying as OES under the NIS Regulations, attainment of the CAF outcomes is mandated. While at this time we do not understand if the person responsible for the asset proposed will be considered an OES. Ofgem encourage the Helios project team look to the guidance provided by the NCSC, to understand practices that would be beneficial to secure the project and consider adopting the measures outlined to manage security risks in the face of growing cyber threat. Building cyber resilience into the project from conception.

The NCSC CAF, and the resources within the CAF collection[6] are intended for the use by organisations that play an important role in the day-to-day life of the UK, organisations such as those designated as forming part of the Critical National Infrastructure (CNI), or organisations subject to certain types of cyber regulation, including The Network & Information Systems (NIS) regulations 2018.

We see the role that large scale batteries and energy storage systems play as becoming increasingly important to the DGE sector and want to encourage uptake of appropriate and proportionate practices as outlined within the CAF collection for new infrastructure projects. This intention aligns with the strategy outlined within the Government consultation on proposals for new legislation to improve the UKs cyber resilience[7]. Whose outcomes[8] are being considered for implementation within the upcoming cyber security and resilience bill[9].

Points of discussion: -

1. Helios Project Representatives comments to Ofgem via email ahead of meeting: –

"Given the multiple sources and diversity of generation in the UK, and the limited generation capacity of the Helios Renewable Energy Project, the project would not meet the National Protective Security Authority ("NPSA") or the UK Governments definition of Critical National Infrastructure ("CNI") or Operator of Essential Services ("OES") so would not be designated as such by the Department for Energy and Net Zero ("DESNZ").

Ofgem's considered response: -

When considered as an independent generation asset the Helios Renewable Energy Project currently falls below the qualification thresholds within Schedule 2 of the NIS Regulation and alone, the asset would not necessitate self-notification under clause 8(2) of the NIS Regulations. However when considered in aggregate with assets owned or operated by affiliated entities the project may yet qualify for nomination through cumulative generation capacity.

Furthermore the Helios Renewable Energy Project may yet be designated as OES by the Secretary of State for Energy Security and Net Zero under clause 8(3) of the Regulations subject to meeting qualifying criteria under clause 8(4) which considers a range of criteria beyond generation capacity alone.

[5] https://www.ncsc.gov.uk/collection/cyber-assessment-framework
[6] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/consolidated-view-of-caf-guidance
[7] https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018
[8] https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience
[9] https://www.gov.uk/government/collections/cyber-security-and-resilience-bill

The Office of Gas and Electricity Markets
9 Millbank London SW1P 3GE **Tel** 020 7901 7000 **Fax** 020 7901 7066 **www.ofgem.gov.uk**

We therefore advise the applicant to continue its engagement with DESNZ to answer any questions that the Secretary of State may have in relation to the project ownership and relationships with other critical infrastructure assets to support any determination of systematic and or systemic risk that could result in designation as OES.

Ofgem drew attention to the need for security practice to be applied to all DGE assets as a matter of considered risk management and that irrespective of NIS Regulations applicability the applicant should be seeking to manage cyber risk as a matter of good practice. This is especially important where security incidents may pose a safety[10], commercial and or environmental risk to the owner and members of the public. This was acknowledged by the project team who explained the diligence applied within its project processes and successful track record of project delivery to design and build infrastructure that is compliant and where required, suitable practice would be adopted…..(continued within point 2).

2. Helios Project Representatives comments to Ofgem (email):-

"The Helios Renewable Energy Project will connect electrically to the National Grid Transmission Network pursuant to an agreement with the National Energy System Operator ("NESO") which (as is standard practice) contains obligations to comply with the required standards and connection conditions set out in the Grid Code, Standard & Quality of Supply Standards ("SQSS") and the Connection and Use of System code ("CUSC").

As such, the project will meet the cyber security standards required of electricity storage and a generating station connecting to the National Electricity Transmission network.

Compliance with these standards and codes means that the project will meet the strict cyber security protocols and firewalls that ensure that NESO's, National Grid's and Elexon's systems, which are designated as CNI, remain secure"

Ofgem's concluding comments: -

(cont.) We acknowledge the application of the codes and standards to support delivery of secure energy infrastructure projects, as highlighted above, mandate the application of minimum obligations for cyber security e.g. the requirement to establish critical tools and facilities that are cyber secure. However, are concerned that many of the clauses within these codes and standards referenced only apply should the responsible party be designated as an OES.

Secondly, we do not see that the codes and standards quoted above provide suitable guidance to support responsible persons as to "how" security practice should be determined and applied. They only outline requirements. Hence the desire to highlight practices recognised by both Ofgem and the UKs technical authority to the applicant.

We encourage Helios to consider how a (cyber) security incident could negatively impact the ability of its network and information systems used to enable or sustain service delivery regardless of NIS compliance thresholds. Of particular concern, we want to draw the applicants attention to precedent cyber security incidents that have the potential for kinetic impacts that could render plant and equipment inoperable and irrecoverable.

We encourage Helios to consult guidance published by the NCSC and other recognised bodies such as energy working groups (Energy Secure Information Exchange (ESIE) and the Energy Network Association (ENA)) to understand better practise that should be followed. Implementing measures to reduce residual risk associated with the occurrence of security incidents effecting its assets sufficiently. And should incidents occur minimising the

[10] https://electrical.theiet.org/guidance-and-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/

The Office of Gas and Electricity Markets
9 Millbank London SW1P 3GE **Tel** 020 7901 7000 **Fax** 020 7901 7066 **www.ofgem.gov.uk**

disruption to the service provided. This is especially important where security incidents pose a significant safety[11], commercial and or environmental risk to the asset and members of the public. Depending upon the nature of the incident, such events could be an initiating event (cause) of further loss of disruption on the wider energy system posing a systemic or systematic risk across the sector. Something we are keen to avoid.

Post discussion with Helios representatives it was acknowledged by the Ofgem team that the project team members are conducting suitable due diligence exercises to increase understanding and awareness of cyber security requirements and importantly that the team have access to suitably qualified and experienced personnel to support the project development moving forward. Although this was not specifically evidenced.

Based on the above understanding between parties and sharing of information both during the course of the meeting and within this follow up response. Ofgem are satisfied with the feedback provided by the third party and do not need to enter a Statement of Common Ground where we have sufficient understanding of the parties intent at this stage and accept the feedback provided. The questions raised by DESNZ however do remain open.

Follow on actions: -

I can confirm that I have incorporated comments received from Stantec against the above and will submit this summary to the The Planning Inspectorate as discussed.

Regards,

[redacted]

Paul Sutton,
Principal OT Security Architect,
Cyber Competent Authority,
Cyber & AI,
Ofgem

[11] https://electrical.theiet.org/guidance-and-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/