

Public

Ref: FOI/25/044

National Energy System Operator

Faraday House

Gallows Hill

Warwick

CV34 6DA

InformationRights@neso.energy

www.neso.energy

30 June 2025

Dear requester

Request for Information

Thank you for your request for information which we received on 2 June 2025. Your request has been considered under the Freedom of Information Act 2000 (FOIA).

Request

You asked us:

Please provide any internal documents, analysis, or discussion notes (whether in draft form or otherwise) from NG ESO / NESO (from 1 January 2022 onwards) relating to:

1. *The anticipated increase in the proportion of system demand met via re-dispatch in the Balancing Mechanism (BM), including:*
 - *Any scenarios or forecasts in which redispatch exceeds 50% of demand by 2030 or earlier (e.g. CP2030 system outlooks).*
 - *Historical benchmarks on BM redispatch volumes (e.g. the original design expectations vs current trends).*
2. *Any internal assessments, risk registers, or third-party reviews addressing the cybersecurity, operational, or system resilience risks of relying on a centralised BM software platform under high redispatch conditions*
 - *Number of EDL / EDT outages listed by month;*

- Any known or recorded SORT system outages, malfunctions or failover events including their duration, cause, and operational impact;
 - Any internal assessments of the criticality of SORT to overall BM functionality, particularly under high-redispach scenarios such as those anticipated under CP2030.
3. Any documents discussing:
- Single points of failure in current BM IT architecture.
 - Planned mitigations, upgrades, or IT redundancy strategies, and their progress versus plan.
 - Dependencies on third-party vendors or proprietary codebases for core BM functionality.
 - The process for balancing the grid if the BM fails

Our response

We confirm that we hold information in scope of your request.

The National Grid Electricity System Operator (NG ESO) was part of the National Grid PLC group of companies until 30 September 2024 and was not subject to the Freedom of Information Act 2000 (FOIA). On 1 October 2024 ('Day 1') we became the National Energy System Operator (NESO) under government ownership (the Independent System Operator and Planner as designated in the Energy Act 2023). Regulation 14 of the Energy Act 2023 (Consequential Amendments) Regulations 2024 (SI 2024/706) amended Part 6 of Schedule 1 (other public bodies and offices: general) of the FOIA, inserting the following: "The Independent System Operator and Planner designated in accordance with section 162 of the Energy Act 2023 in respect of information held by it as a result of the exercise of its functions under, or as a consequence of, that Act." NESO has therefore been subject to the FOIA since 1 October 2024 and may refuse FOIA requests in respect of information collected, received, or created prior to Day 1.

Our obligation is to provide you with information held up to the date we received your request however, in the interest of providing as much up to date information as possible we are providing information which was published as recently as the 16 June 2025.

In response to question 1, NESO have recently published 2025 [Annual Balancing Costs Report](#) providing a look back on recent balancing trends and drivers as well as a broad view of potential future balancing costs addressing NESO's role in minimising costs. The report shows at least £1.2 bn of consumer benefit in the last two years.

The Strategy has been developed to minimise rising costs by leveraging initiatives in:

1. Network planning and optimisation

2. Commercial mechanisms
3. Research, innovation, and engagement
4. Control room processes

NESO's 2025 [Strategy Report](#) describes 4 phases of its roadmap, recaps our Phase 1 strategy and introduces our Phase 2 strategy (Monitoring and Implementation Phase), starting from 2025. We also consider how this strategy will need to evolve over the longer term to accommodate the future power system.

In response to questions 2 & 3, NESO recently published its 2025 [Frequency Risk and Control Report](#) which includes an assessment of the magnitude, duration and likelihood of transient frequency deviations, forecast impact and the cost of securing the system and confirms which risks will or will not be secured operationally.

At NESO security of supply is at the heart of everything we do and is our number one priority, as shown by our 2023-24 reliability of supply being 99.99999%. Alongside this, NESO has also initiated a number of [strategic projects](#), including but not limited to resource adequacy, assessing the potential risks to security of supply and whether there are sufficient available resources to meet electricity demand throughout the year.

NESO are at the forefront of innovation researching the current and projected cybersecurity threat to the energy sector further, being awarded Alpha phase funding to progress to Alpha phase development with its innovative project on Network Security in a Quantum Future, building on the completed and successful delivery of the Discovery phase in May 2024. [SIF R3 Alpha: Network Security in a Quantum Future | National Energy System Operator](#). The Network Security in a Quantum Future project will create an innovative risk management tool to assess the quantum threat to the energy network, mapping it to a diverse range of energy assets, and enabling prioritisation of mitigations.

In accordance with: Section 31(1)(a) (prevention or detection of crime) of the FOIA

Further information you have requested in questions 2 & 3 is refused in accordance with s31(1)(a) of the Freedom of Information Act (FOIA) for the reasons stated below. Cyberattacks may amount to criminal offences under s3 of the Computer Misuse Act 1990 and or s170-173 of the Data Protection Act 2018. As you have requested the information under the FOIA, consideration has to be given to the fact that the legislation is applicant blind. As a result, any disclosure has to be treated as if it was being sent to the world at large as opposed to a specific individual when considering the harm in disclosure. NESO therefore has to take account of the wide range of

individuals, groups, and even sovereign states that may use information about NESO to facilitate cyber-crimes.

As part of the UK's critical national infrastructure (CNI), the energy system must be secure against malicious cyberattacks. NESO works collaboratively with OFGEM, DESNZ, private sector partners and other government agencies whilst also participating in innovative research to identify, understand and mitigate against vulnerabilities and risks to ensure the appropriate technical and organisational safeguarding measures are in place. The organic nature of the global threat and attack vector requires NESO to assess all known threat intelligence in a secure safe space whilst ensuring the security of supply to GB at all times.

NESO works with multiple agencies and operators ensuring the security of supply. The resilience of the network is paramount and is constantly tested by persistent and evolving cyber threats. Cyber-attacks are rated as a Tier 1 threat by the UK Government and evidenced in the recently published [National Security Strategy 2025](#) addressing the very real and heightened threats facing the UK including its CNI. It is recognised the emergence of state-aligned actors as a new and emerging cyber threat to CNI has been exacerbated by Russia's full-scale invasion of Ukraine and hostilities in the Middle East. As energy underpins every part of our society, any threats or successful cyber-attacks to our energy supply can have serious consequences for essential services, potentially putting lives at risk. Disclosure of the requested information would make it easier for malicious actors to find and exploit potential vulnerabilities, and would be likely to risk the integrity of the network to the detriment of GB.

Public Interest Test

This exemption is a qualified exemption which requires a public interest test. NESO recognises there is a general public interest in disclosure of information that would promote transparency of the requested information. This includes information about the vulnerabilities and risks relating to the security of supply and resilience of the network. NESO must balance its transparency obligations with protecting the resilience of the network and the security of supply. In this case, NESO does not consider that the public interest in transparency is sufficiently strong enough to outweigh the substantial interest in maintaining the integrity of the network for the reasons stated above. In our opinion, the public interest is sufficiently met by the abundance of [industry data and reports](#), [publications](#) which NESO issues as well as our weekly engagement via NESO's [Operational Transparency Forum](#), an open technical industry forum discussing recent operational actions with a live Q&A session.

Evidence of Harm

As stated above, the FOIA is applicant blind therefore disclosure to one requester who may be a genuine and interested person is also by default a disclosure to the world at large, placing the requested information into the public domain could cause considerable harm if it was used to attack the security of supply and resilience of the network. It is a recognised fact the UK CNI are a prime target and under persistent attack from individual and state attackers, now more than ever we need to ensure our CNI is protected. Effective planning and operating of our increasingly complex energy system requires consideration of the interactions across electricity, gas and other forms of energy. NESO also needs to consider the interdependencies with other sectors, such as water, transport, telecommunications and industry. Disclosure of the requested information in questions 2&3 would impact NESO's ability to operate, plan, manage and mitigate against risks to the security of supply and resilience of the network.

This concludes our response to your request.

Next steps

If you are dissatisfied with our handling of your request, you can ask us to review our response. If you want us to carry out a review, please let us know within 40 working days and quote the reference number at the top of this letter. You can find our procedure here: [Freedom of Information and Environmental Information Regulations | National Energy System Operator](#). The ICO's website also provides guidance on the internal review process: [What to do if you are dissatisfied with the response | ICO](#).

If you are still dissatisfied after our internal review, you can complain to the Information Commissioner's Office (ICO). You should make complaints to the ICO within six weeks of receiving the outcome of an internal review. The easiest way to lodge a complaint is through their website: www.ico.org.uk/foicomplaints. Alternatively, they can be contacted at: Wycliffe House, Water Lane, Wilmslow, SK9 5AF.

Thank you for your interest in the work of the National Energy System Operator (NESO).

Regards,

The Information Rights Team, National Energy System Operator (NESO)