National Cyber Security Policy Consultation
Dept of Environment, Climate and Communications
29-31 Adelaide Road
Dublin 2
D02 X285

January 31, 2023

To whom it concerns,

As an Operator of Essential Services under the current Network and Information Systems Directive ('NIS-D') framework, Aer Lingus welcomes the opportunity to participate in this consultation process on the National Cybersecurity Strategy Mid-Term Review.

Aer Lingus supports the additional measures put forward by the National Cyber Security Centre (NCSC) as part of the strategic review as included in the consultation documentation, and welcome in particular:

- The proposal in **Section 7** to build a network of sectoral Information Sharing Networks, backed by a secure Cyber Threat Intelligence sharing platform

- The additional measures in **Section 9** to continue the development of cybersecurity skills throughout the economy including the creation of a National Cyber Security Centre Support Centre to promote awareness of resources for improving cybersecurity capabilities.

- The continued development of national cybersecurity information campaigns detailed in **Section 12** to raise awareness of cyber risks including phishing and ransomware.

In addition, Aer Lingus would like to propose the following additional amendments that could support the strengthening the proposed National Cybersecurity Strategy:

Aer Lingus believes that coordinated engagement with Operators of Essential Services (OES), as a critical stakeholder group, should be represented in the **Vision** statement.

On this basis Aer Lingus proposes the following alternative wording: "**Engage** nationally and internationally in a strategic, and *co-ordinated* manner, supporting a free, open, peaceful and secure cyber space, and ensuring that cyber security is a key component of *Ireland's diplomatic, economic and regulatory* posture across the full range of engagement."

Under the current Vision objectives, Aer Lingus believe that an opportunity exists to extend references to the response readiness of OES to include "*protect, detect and respond*". Aer Lingus believes that this would be a more appropriate inclusion and provides recognition of the OES contribution to and investment in national cyber security.

Under the National Capacity Development section, Aer Lingus recommends extending the proposal 6, bullet point 3, to include reference *to "capacity building measures to support the development of 1) a service catalogue for the NCSC to support organisations including OES's; and 2) a target governance model for individual OES's to engage with the NCSC"*

Aer Lingus believes that this amendment would provide a specific measure where joint responsibilities and efforts can be coordinated to ensure NCSC capacity building supports OES engagement.

On Governance Framework & Responsibilities, Aer Lingus recommends extending proposal 13 to incorporate an additional point 2 as follows: *"Advisory Group to be drawn down from operators of essential services to ensure the continued evolution and harmonisation of a governance framework and responsibilities, in a manner that is proportionate and reflects any wider governance or regulatory frameworks that such operators are currently subject to"*

This would ensure overlapping governance such as aviation security is considered, as well as ensuring effective, proportionate governance control design and engagement protocols.

Aer Lingus will continue to positively engage with the NCSC providing ongoing feedback as part of the current engagement model, including highlighting continuous improvement opportunities that balance formal and informal notification processes with drawdown of advisory services and NCSC expertise.

We remain available to discuss any aspects of our submission as required.

Sincerely,

Director Corporate Affairs