Cabinet Secretary for Justice and Home Affairs
Angela Constance MSP

F/T: 0300 244 4000
E: scottish.ministers@gov.scot

Scottish Government
Riaghaltas na h-Alba

Michelle Thomson MSP
Deputy Convener
Economy and Fair Work Committee
The Scottish Parliament
Edinburgh
EH99 1SP

By email:
economyandfairwork.committee@parliament.scot

24 March 2026

Dear Deputy Convener,

**CYBER SECURITY AND RESILIENCE (NETWORK AND INFORMATION SYSTEMS) BILL**

Thank you for the opportunity to discuss the UK Cyber Security and Resilience Bill with the Economy and Fair Work Committee at the session on 4 March. I trust that the evidence provided by my officials and I have been helpful in explaining the subtleties of the legislation, challenges with cyber security and the ongoing activities to improve the cyber resilience of Scotland.

You asked a final question at the end of the session regarding how cyber in general is managed in government. Unfortunately, time did not allow a complete answer to this question so I am providing an overview below of the current structures within Scottish Government that work together to ensure cyber matters are considered appropriately.

**Overview of Cyber Security and Resilience in Scottish Government**

Resilience in general falls within my remit as Cabinet Secretary for Justice and Home Affairs and this includes cyber resilience. The **National Cyber Security and Resilience Division (NCSR)** leads on cyber security and resilience matters, and this sits within the Digital Directorate. There are three units within the NCSR Division:

- **Cyber Resilience Unit (CRU)** - The CRU are the policy team which develops and maintains the Strategic Framework for a Cyber Resilient Scotland (November 2025) and oversees its implementation through the Action plan (published last month). The CRU also provides Secretariat support to the National Cyber Resilience Advisory Board which provides strategic advice, challenge and support to Scottish Ministers and the Scottish Government on cyber resilience matters. The CRU works with policy

teams across the Scottish Government to ensure that cyber resilience and security considerations are taken into account as government policies and strategies are being developed. The CRU also hosts Public Sector Cyber Resilience Network webinars which regularly bring together the cyber/information security professionals across the sector to share good practice, lessons from exercises and incidents, latest threat intelligence and policy developments.

- **Cyber Security Unit (CSU)** - The CSU are the cyber and information security professionals that ensure Scottish Government's own cyber risks are managed appropriately and that government systems and procedures are cyber secure and resilient. Their remit also covers aspects of the cyber security of more than 50 Scottish public bodies which make use of Scottish Government networks and devices. The CSU also works closely with the Security and Business Continuity Division as part of a holistic approach to security within Scottish Government.

- **The Scottish Cyber Coordination Centre (SC3)** - SC3 was established in 2021 to provide a central function to combat the accelerating cyber threat. SC3 supports the public sector with threat intelligence, vulnerability management, cyber exercising and standards and insight.
  In addition, SC3 maintains a 24/7 capability to help support incident coordination for any public sector organisations that suffers a significant cyber incident.

I hope you find this information useful and I look forward to updating the Committee in the future as the Cyber Security and Resilience Bill progresses.

Yours sincerely,

**ANGELA CONSTANCE**



St Andrew's House, Regent Road, Edinburgh EH1 3DG
www.gov.scot