Cabinet Secretary for the Rural Economy and Connectivity
Fergus Ewing MSP

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

Scottish Government
Riaghaltas na h-Alba
gov.scot

Edward Mountain MSP
Convener
Rural Economy and Connectivity Committee
Scottish Parliament
EDINBURGH
EH99 1SP

6 March 2018

Dear Edward,

This letter provides further detail on a number of issues that were briefly discussed during my appearance at the REC committee session on 31 January.

R100 Procurement

The initial R100 procurement is being run as a competitive dialogue and these generally take between 12-18 months to complete. The contract notice was issued in December 2017 and the market interest it has generated is entirely in line with our expectations. The level of ambition, and funding, that we have set out has attracted a range of bidders.

We have just completed our shortlisting exercise of those bidders who will progress to the tender stage and will issue an Invitation to Participate in Dialogue (tender documents) to them shortly. The bidders through to the next stage are:

- Axione
- British Telecommunications plc
- Gigaclear plc
- SSE Telecommunications Ltd.

We are confident that we will have suppliers in place – and ready to deploy – by early 2019, avoiding any significant gap between DSSB ending and R100 starting.

The coverage footprint to be delivered by the initial R100 procurement will only be confirmed at the end of the procurement process. The procurement is specifically designed, however, to ensure that new fibre backhaul is extended to all corners of the country. This will provide the platform for a range of aligned interventions, which will bring superfast broadband to any premises not reached by the initial procurement. We will look to clearly communicate the precise detail as early as possible to the public, so that they can understand what infrastructure will be deployed in their area and when.

Rather than one national lot, we have split the procurement into 3 regional lots to give us the best possible chance of maximising competition – driving value and innovation. This was informed by extensive engagement with the market during 2017. A single, national lot would have favoured a very small number of suppliers. We wanted to ensure that smaller companies – albeit ones that have a proven track record of delivering at scale – are able to bid competitively.

We also plan to make delivery of gigabit infrastructure in challenging rural locations a requirement of the North lot, ensuring that gaps in fibre provision are filled. These locations will be confirmed shortly, once we have confirmation of the final coverage footprint to be delivered by the DSSB programme.

This procurement will focus on around 180,000 premises – the majority of which are in the North lot. We have taken the decision not to focus on urban city centre premises in this first phase but to target investment where it is needed most – in rural Scotland. We expect commercial suppliers to fill gaps in urban areas and recent announcements from the likes of BT, CityFibre and Vodafone, suggests that this approach is the right one.

As I am sure you can appreciate, we are limited by commercial confidentiality on what we can share publicly with the Committee at this stage of the procurement but I would be happy to offer a further informal briefing with my officials if helpful.

Building Standards

Our building standards system is set up to cover how individual buildings can function when initially constructed. It has tended not to be used to address matters that require a strategic overview across the entire country or local authority areas, such as rollout of broadband infrastructure, or utilities in general. A building warrant is one of the last permissions sought, after all other key strategic development decisions have been taken. Indeed, most utilities infrastructure is exempt from building regulations (and consequently a warrant) which helps to secure its delivery in an expedited manner.

In view of this, the building standards system does not require any utilities (namely gas, water, electric or telecommunications) to be provided to any new building. However, since the beginning of 2017 our building regulations require a route to be formed, for broadband services, through the external wall into a new building and to each subsequent building unit (for multi-occupation buildings such as flats).

This provision will assist with the roll-out of broadband services when building owners elect to carry out such installation, not only when buildings are new, but also during the life of such buildings.

Planning

Our national planning policies are supportive of digital connectivity and are helping to enable the delivery of the infrastructure needed to support the growth of broadband across Scotland. Planning authorities should adhere to and utilise the approaches advocated in Scottish Planning Policy (SPP) and National Planning Framework 3 (NPF3) when preparing their development plans.

Currently, SPP encourages developers to agree with infrastructure providers to build in coverage and capacity to new developments. SPP sets out that "Policies should encourage developers to explore opportunities for the provision of digital infrastructure to new homes and business premises as an integral part of development. This should be done in consultation with service providers so that appropriate, universal and future-proofed infrastructure is installed and utilised."

One of the key themes of NPF3 is "A Connected Place". NPF3 sets out proposals for digital connectivity enhancement in city regions, rural areas and coastal and island communities further supplementing the support given through the planning system.

The Planning Review Position Statement (June 2017) highlighted that options for a delivery group, to improve the co-ordination of development and infrastructure, were being considered. This has now been taken forward, with the first meeting of the Infrastructure Delivery Group held on 6th November 2017. This was well attended by a wide range of infrastructure providers, including digital, with the aim of improving communication and co-ordination around the development planning process. Topics discussed included how the organisations engage with the planning system and current barriers to involvement and alignment with planning. The next meeting of the group will be held on 5th March 2018..

We can also consider the need to further enhance, or modify, the planning system to support digital and broadband infrastructure through planning policies when we next review SPP and NPF. This would be carried out through full consultation with all relevant stakeholders. Our Planning Bill seeks to enhance the status of the NPF, incorporating the SPP, as part of the statutory development plan.

Whilst the above measures set out those ways in which planning can, and will continue to take, an active role in supporting the delivery of digital infrastructure across Scotland, I should also explain that the planning system cannot *require* delivery of infrastructure by third parties. Whilst it is open to planning authorities when granting planning permission to impose conditions to make the development acceptable in planning terms, there are constraints on the use of such conditions.

For example, planning authorities could not use conditions to compel a third party (such as a communications infrastructure provider) to connect to or adopt infrastructure provided by a developer. Nor could a condition require a developer to enter into an agreement with a third party to provide infrastructure.

Cyber Resilience

The Scottish Government fully recognises the seriousness of the cyber threat, which was emphasised by the impact of the Wannacry attack on the NHS in Scotland and England in May 2017.

Legislative developments (GDPR and NIS)

The General Data Protection Regulation (GDPR) will also come into force in in May 2018. As part of wider protections for personal data, this will include requirements for appropriate technical security.

The new Security of Network and Information Systems (NIS) Directive will apply in Scotland and the rest of the UK from May 2018, and places cyber resilience requirements on operators of some essential services (including energy, transport, healthcare and water). Under the NIS Directive the cyber resilience of essential services will be regulated by Competent Authorities. Competent Authorities will be established in Scotland for devolved essential services, which will include the Scottish health sector. The Scottish Government is working closely with the UK Government to ensure the Directive is implemented appropriately in Scotland.

Strategy and action plans

Scotland's cyber resilience strategy, "Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland" was published in 2015, and sets an ambition for Scotland to become a world leading nation in cyber resilience.

The 2017-18 Programme for Government committed the Scottish Government to working with the National Cyber Resilience Leaders' Board (NCRLB – a cross-sectoral group of leaders and experts in cyber resilience) to develop and implement a suite of 5 action plans to help Scotland to achieve that ambition.

Public sector work

The first of these, the Public Sector Action Plan on Cyber Resilience for Scotland (PSAP), was launched in November 2017 by the Deputy First Minister. It aims to promote a common approach to cyber resilience across Scotland's public sector. It includes a range of key actions and support for Scottish public bodies around robust cyber governance arrangements, active threat intelligence sharing, clear cyber incident response protocols, and independent assurance of critical technical controls to defend against the most common cyber-attacks. If successfully implemented, we believe the PSAP will make Scotland the first UK nation to achieve these goals across all of our public bodies.

The PSAP applies to public bodies, but we are also working with universities and colleges and local authorities to ensure an aligned approach across the wider Scottish public sector wherever possible. We will also work closely with Health Boards and the new NIS Competent Authorities (once established) on the applicability of the action plan in the context of the NIS Directive's requirements.

The Scottish Government has spent £5 million from 2015-18 to strengthen its own cyber security arrangements, and is currently undergoing certification to Cyber Essentials Plus level, in line with the requirements of the PSAP.

Other action plans

Beyond the public sector, we are currently working with the NCRLB and sector leads to develop complementary action plans for Scotland's private and third sectors, and we are developing a Learning and Skills Action Plan to ensure our young people can operate confidently online and have opportunities to develop cyber specialist skills. The learning and skills action plan is expected to be published shortly.

We are working with Scottish Enterprise and other partners to develop an Economic Opportunity Action Plan to support innovation and research in cyber security.

The Scottish Government has allocated £1 million in support of these action plans during 2018-19.

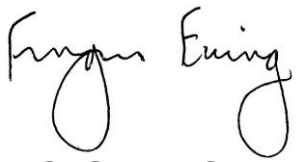
National Cyber Security Programme Funding for Scotland

Around £6.5 million over the current and next three years has been allocated to Scotland from the National Cyber Security Programme fund to support the implementation of the UK Government's Strategy, and in turn the Scottish Government's Cyber Resilience Strategy for Scotland. In 2017-18, a total of £1.3 million of this funding was allocated to a range of projects to build cyber resilience within workplaces, schools, universities and the third sector, and there are currently 20 projects underway in Scotland.

These cover a broad range of initiatives to improve and build on Scotland's cyber resilience including: in-depth analysis of the scale and impact of cyber-crime in Scotland; projects to promote and support the take-up of Cyber Essentials across all sectors; development of educational resources and qualifications in cyber subjects; awareness raising campaigns around general cyber resilience as well as the promotion of career opportunities in cyber security for youth audiences; raising awareness of cyber security in the workplace; and increasing PROTECT capability within Police Scotland to support organisations across Scotland to raise awareness of cyber risks and promote good practice in their communities.

I trust this information is useful.

Yours sincerely,



FERGUS EWING