

Performance update – moving ahead in 2020

Our previous performance updates explain how the recruitment of additional inspectors, the implementation of the Rosewell Review recommendations and the new planning appeals portal are helping us improve appeal handling times and provide a much better customer service.

We are continuing to make progress and make changes which will help deliver the service our customers expect.

Planning appeals

We are continuing to improve the time taken to decide appeals. For appeals handled through written representations the average time for decision currently stands at 19 weeks; 10 weeks less than the time taken in January 2019. Historic Heritage casework was an area where appeals were consistently taking longer to determine. To improve this, we have increased the number of Inspectors who are able to deal with this type of specialist casework.

We are also making good progress with clearing older hearing cases. The number of live hearing appeals has reduced every month for the last six months. The median decision time is now 32 weeks compared to a high of 47 weeks over the summer of 2019. The valid-to-start data for hearings shows

Enforcement

Performance is improving for Enforcement appeals with the number of decisions issued increasing in the last three months. This is as a result of the additional Inspectors who have been trained to undertake this type of casework. The time for new cases to be assessed for validity is on average 2 weeks and the waiting time for written representations appeals to be started has reduced significantly. This means that written representation appeals submitted now are likely to hit the valid-to-decision target of 36 weeks.

Our focus is now on handling times for Enforcement hearings and inquiries. We are expecting to see an improvement in this area later this year.

Rosewell Review

Following the [Rosewell Review](#), which was published on 12th February 2019, 15 of the 22 recommendations are now implemented.

We are holding a 'One year on event' in February for parties involved in the Review and its implementation, to consider what has gone well and where further focus is still required. We will also publish another update of the

Action Plan at the beginning of March. This will provide details on the progress made to date and planned improvements for the remainder of this year.

All Inspector decided inquiry planning appeals submitted to the Inspectorate since 1 April 2019 have followed the Rosewell timing recommendations. All except one were decided in fewer than 26 weeks. On average the cases took 22 weeks to decide and 10 were decided in 20 weeks or fewer.

As we continue to improve our guidance, we have produced the following [video for Rule 6 parties](#). Narrated by our senior Inspector, Jenny Vyse, the video answers questions most commonly asked and talks through the process of how to become a Rule 6 party.

Cases for Decision by Secretary of State

Following the successful implementation of many of the recommendations in the Rosewell review for Section 78 appeals and the publication of our updated Action Plan in October 2019, we have started looking into ways of implementing some of the Rosewell recommendations for the processing of called in planning applications. From now on we will work with those applicants whose applications are called in and the local planning authorities involved. This moves away from our “bespoke” process where we would have invited the parties to agree a programme, including an inquiry date.

This is the next step in significantly shortening the delays in arranging planning inquiries, and will speed up the time from when the application is called in to the issue of the Secretary of State’s decision. In the meantime we will not be able to “bring forward” inquiries already arranged, and the previously agreed bespoke programmes in those cases will continue to apply. Our [published Guidance](#) will be updated as we move forward with this work.

Local Development Plans

There were 43 local plans submitted to the Planning Inspectorate in 2019 with 59 final Inspector reports issued in the year, all of which found the plans sound. 2 local plans were withdrawn in 2019. There are currently 77 local plans in progress.

National Infrastructure Planning

We currently have 30 live cases (15 energy and 15 transport). These include the longest linear Nationally Significant Infrastructure Project (NSIP) examined (Southampton to London Pipeline Project), the first solar NSIP (Cleve Hill Solar Park), the first interconnector (Aquind) and our first consideration of separate, simultaneous applications (East Anglia 1 North and East Anglia 2).

We are also expecting some 30 projects in 2020. These include substantial cases such as Sizewell C Nuclear Power Station, Lower Thames Crossing, Luton

Airport and the expansion of Heathrow Airport. The Inspectorate has met all its statutory deadlines for National Infrastructure and submitted 16 recommendation reports to the relevant Secretaries of State over the course of 2019.

Making it easier to submit an appeal

Work to improve the Appeal Casework Portal is continuing. The Beta phase continues to gather important information from users to help us refine the system currently in development. We have received 132 appeals through the new Portal, 26 of which have progressed all the way through to the decisions being issued. The project team are currently working on developing the functionality to allow linking of multiple appeals for the same development appeals and building the functionality to process other appeal types such as Technical Design Consent & Permission in Principle. Alongside this a steady flow of continuous improvements are being made to the system based on the valuable feedback already received.

Baroness Morgan's Oral Statement on UK Telecommunications

My Noble Lords, with leave, I will make a statement on the security of the telecoms supply chain

This Government is committed to securing nationwide coverage of gigabit-capable broadband by 2025.

Because we know the benefits that world-class connectivity can bring.

From empowering rural businesses...

To enabling closer relationships for the socially isolated...

To new possibilities for our manufacturing and transport industries.

We are removing the barriers to faster network deployment and have committed five billion pounds of new public funding to ensure no area is left behind.

It is, of course, essential that these new networks are secure and resilient. That is why the Government has undertaken a comprehensive review of the supply arrangements for 5G and full fibre networks.

Telecoms Supply Chain Review

The Telecoms Supply Chain Review – laid in the Other Place in July last year – underlined the range and nature of the risks facing our critical digital

infrastructure – from espionage and sabotage to destructive cyber attacks.

We have looked at the issue of how to maintain network security and resilience over many months and in great technical detail.

We would never take decisions that threaten our national security or the security of our Five Eyes partners.

As a result, the technical and security analysis undertaken by GCHQ's National Cyber Security Centre is central to the conclusions of the Review. Thanks to their analysis we have the most detailed study of what is needed to protect 5G, anywhere in the world.

It is also because of the work of the Huawei Cyber Security Evaluation Centre Oversight Board, established by NCSC, that we know more about Huawei, and the risks it poses, than any other country.

We are now taking forward the Review's recommendations in three areas.

World-leading regulation

First, world leading regulation.

We are establishing one of the strongest regimes for telecoms security in the world – a regime that will raise security standards across the UK's telecoms operators and the vendors that supply them.

At the heart of the new regime, the NCSC's new Telecoms Security Requirements guidance will provide clarity to industry on what is expected in terms of network security.

The TSRs will raise the height of the security bar and set out tough new standards to be met in the design and operation of the UK's telecoms networks.

The Government intends to legislate at the earliest opportunity to introduce a new comprehensive telecoms security regime – to be overseen by the regulator, Ofcom, and Government.

Market diversification

Second, the Review also underlined the need for the UK to improve diversity in the supply of equipment to telecoms networks.

Currently, the UK faces a choice of only three major players to supply key parts of our telecoms networks.

This has implications for the security and resilience of these networks, as well as for future innovation and market capacity. It is a 'market failure' that needs to be addressed.

The Government is developing an ambitious strategy to help diversify that supply chain. This will entail the deployment of all the tools at the

Government's disposal, including funding.

We will do three things simultaneously:

We will seek to attract established vendors who are not present in the UK, to our country...

We will support the emergence of new, disruptive entrants to the supply chain...

And we will promote the adoption of open, interoperable standards that will reduce barriers to entry...

The UK's operators are leading the world in the adoption of new, innovative approaches to expand the supply chain.

The Government will work with industry to seize these opportunities.

And we will also partner with like-minded countries to diversify the telecoms market.

Because it is essential that we are never again in a position of having limited choices when deploying important new technologies.

High Risk Vendors

The third area covered by the Review was how to treat those vendors which pose greater security and resilience risks to UK telecoms.

As I know the House has a particular interest in this area, I will cover this recommendation in detail.

Those risks may arise from technical deficiencies or considerations relating to the ownership and operating location of the vendor.

As noble Lords may recall, the Government informed the Other Place in July that it was not in a position to announce a decision on this aspect of the Review.

We have now completed our consideration of all the information and analysis – from the National Cyber Security Centre, industry and our international partners.

And today, I am able to announce the final conclusions of the Telecoms Supply Chain Review in relation to high risk vendors.

In order to assess a vendor as high risk, the Review recommends a set of objective factors are taken into account. These include:

- the strategic position or scale of the vendor in the UK network...
- the strategic position or scale of the vendor in other telecoms

networks, particularly if the vendor is new to the UK market...

- the quality and transparency of the vendor's engineering practices and cyber security controls...
- the vendor's resilience both in technical terms and in relation to the continuity of supply to UK operators...
- the vendor's domestic security laws in the jurisdiction where the vendor is based and the risk of external direction that conflicts with UK law...
- the relationship between the vendor and the vendor's domestic state apparatus...

And finally, the availability of offensive cyber capability by that domestic state apparatus, or associated actors, that might be used to target UK interests.

New controls on high risk vendors

To ensure the security of 5G and full fibre networks, it is both necessary and proportionate to place tight restrictions on the presence of any companies identified as higher risk.

The debate is not just about 'the core' and 'the edge' of networks. Neither is it just about trusted and untrusted vendors.

Threats to our networks are many and varied, whether from cyber criminals or state sponsored malicious cyber activity.

The most serious recent attack on UK telecoms has come from Russia, and there is no Russian equipment in our networks.

The reality is that these are highly complicated networks relying on global supply chains, where some limited measure of vulnerability is inevitable.

The critical security question is: how to mitigate such vulnerabilities and stop them damaging the British people and our economy?

For 5G and full fibre networks, the Review concluded that, based on the current position of the UK market, high risk vendors should be:

Excluded from all safety related and safety critical networks in Critical National Infrastructure...

Excluded from security critical network functions...

Limited to a minority presence in other network functions up to a cap of 35 per cent...

And be subjected to tight restrictions, including exclusions from sensitive geographic locations.

These new controls are also contingent on an NCSC-approved risk mitigation strategy for any operator who uses such a vendor.

We will legislate at the earliest opportunity to limit and control the presence of high risk vendors in the UK network, and to allow us to respond as technology changes.

Over time, our intention is for the market share of high risk vendors to reduce as market diversification takes place.

I also want to be clear that nothing in the Review affects this country's ability to share highly sensitive intelligence data over highly secure networks, both within the U.K. and with our partners, including the Five Eyes.

GCHQ has categorically confirmed that how we construct our 5G and full fibre public telecoms networks has nothing to do with how we share classified data.

And the UK's technical security experts have agreed that the new controls on high risk vendors are completely consistent with the UK's security needs.

NCSC industry advice

In response to the Review's conclusions on high risk vendors, the Government has asked NCSC to produce guidance for industry. This guidance was published earlier today on the NCSC's website.

The NCSC has helped operators manage the use of vendors that pose a greater national security risk, such as Huawei and ZTE, for many years.

This new guidance will include how it determines whether a vendor is high risk...

The precise restrictions it advises should be applied to high risk vendors in the UK's 5G and full fibre networks...

And what mitigation measures operators should take if using high risk vendors.

As with other advice from the NCSC on cyber security matters, this advice will be in the form of guidance.

The Government expects UK telecoms operators to give due consideration to this advice, as they do with all their interactions with the NCSC.

Conclusion

I hope the whole House will agree that if we are to achieve our digital connectivity ambitions, it is imperative that we trust the safety and security of our telecom networks.

Risk cannot be eliminated in telecoms.

But it is the job of Government, Ofcom and industry to work together to ensure that we reduce our vulnerabilities and mitigate the risks.

This Government's position on high risk vendors marks a major change in the UK's approach.

When taken together with the tough new security standards that will apply to operators, this approach will substantially improve the security and resilience of the UK's telecoms networks, which are a critical part of our national infrastructure.

It reflects the maturity of the UK's market and our world-leading cyber security expertise, and follows a rigorous and evidenced-based review. It is the right decision for the UK's specific circumstances.

The future of our digital economy depends on trust in its safety and security.

And if we are to encourage the takeup of new technologies that will transform our lives for the better then we need to have the right measures in place.

That is what this new framework will deliver and I commend this statement to the House.

[Serial immigration fraudster jailed for longer](#)

A man who forged documents to support immigration visa applications has had his sentence increased by the Court of Appeal following intervention by the Solicitor General, the Rt Hon Michael Ellis QC MP.

From 2013 to 2017 Mohammad Rahman took part in a number of fraudulent schemes, including supplying false documents designed to support immigration visa applications, and fake student council tax exemptions.

As part of the scam, Rahman produced false documents purporting to be from educational institutions to allow overseas nationals to reside in the UK for the purpose of study, having supposedly secured a place on a course.

Other fraudulent schemes run by Rahman included creating false documentation to secure council tax exemptions for people claiming to be enrolled in courses and falsifying documents which allowed his wife and sister-in-law to secure a mortgage advance of over £140,000 to purchase a house.

When immigration officers attended the offender's workplace, he was found in

possession of a memory stick loaded with hundreds of false documents, templates and fake correspondence from legitimate educational institutions.

On 21 November 2019, Rahman was sentenced at Kingston Crown Court to 2 years and 6 months' imprisonment.

Today the Court of Appeal increased this to 5 years' imprisonment, after the sentence was referred as being unduly lenient by the Solicitor General, the Rt Hon Michael Ellis QC MP.

After the hearing the Solicitor General said:

"The offender set out to make substantial financial gain from dishonest activity in which he abused his position of responsibility. He continued to disregard the law and the victims of his crimes and this increase in sentence is wholly appropriate."

[UK and EEA EFTA States sign Separation Agreement](#)

The UK, Norway, Iceland and Liechtenstein have today signed the EEA EFTA Separation Agreement. This agreement largely mirrors the Withdrawal Agreement negotiated with the EU.

The agreement protects the rights of 17,000 UK nationals living in the EEA EFTA States and 15,000 EEA EFTA nationals living in the UK, ensuring that at the end of the Transition Period they will be able to enjoy broadly the same rights as they do now. It also resolves a small number of other issues arising from the UK's exit from the EU.

Brexit Secretary Steve Barclay signed the agreement on behalf of the UK, alongside representatives of Norway, Iceland and Liechtenstein.

Mr Barclay said: "This agreement underlines the importance of our relationships with our close friends and allies in the EEA EFTA states.

"It will protect the rights of citizens and provide certainty to business as the UK leaves the EU, ensuring an orderly withdrawal and smooth transition as we put in place new arrangements for our future relationship with the EEA EFTA States."

This agreement was first [announced](#) and [published](#) in draft on 20 December 2018 and today (28 January 2020) marks the formal signing.

Further information:

[EEA EFTA Separation Agreement and Explainer](#)

[New guide helps find and classify geospatial datasets across search engines](#)

The Geospatial Commission and its six partner bodies have released [Search Engine Optimisation \(SEO\) for publishers: Best practice guide](#) to make it easier to find and classify geospatial datasets across all search engines.

This is the second in the series of guides to improve discovery and usability of geospatial data, after the publication of the [Linked identifier schemes: Best practice guide](#) last year.

The guide has been created because most users seek out geospatial data using common search engines and at the moment these are not necessarily finding or prioritising the authoritative national datasets. By following the tips in the guide data publishers can make their data easier to find by users who can then devote more of their time to joining it with other data sets and carrying out analysis to provide insight and support better decision making.

Thalia Baldwin, Geospatial Commission Director, said

Again, our Partner Bodies are working collaboratively and drawing on their network of peers across government to produce a new guide that will help to make a real difference to how easily geospatial data can be found. This guide sits alongside the first one we published on Linked Identifiers and together they provide a valuable resource for data publishers who are interested in increasing the use and value of their data.

Shona Nicol, Head of Data Standards, Scottish Government, added:

By implementing these recommendations data publishers stand to benefit from increased visibility of their data among a wider audience, while people wanting to use geospatial data are more likely to find what they are looking for. For example, by using this guide the Scottish Government has already identified that its webpages are not being optimally indexed by search engines because they are not tagged using the industry-standard markup language Schema.org. By making this change the Scottish Government will dramatically increase the chances of potential users finding its

data.

The Geospatial Commission would welcome feedback on its guides. If you would like to participate please contact geospatialcommission@cabinetoffice.gov.uk.