Separated migrant children to access legal aid more easily

Draft legislation will bring immigration and citizenship matters into the scope of legal aid for separated migrant children.

Published 22 July 2019 From: Ministry of Justice



- Immigration matters for separated migrant children to be brought into scope of legal aid
- Support will be quicker and easier to access
- Access to justice will be improved for these vulnerable children

Draft legislation laid in parliament today will make it easier for separated migrant children to apply for legal aid.

Once approved by both houses, the change will ensure some of society's most vulnerable children can more quickly secure legal advice and representation by bringing immigration and citizenship matters into the scope of legal aid for under 18s who are not in the care of a parent or guardian, or who are looked after by a local authority.

Previously, separated migrant children making non-asylum immigration applications to remain in the UK would have been required to apply for legal aid through the Exceptional Case Funding (ECF) scheme. This is intended to ensure legal aid is accessible in all cases where there is a breach or risk of a breach of the European Convention on Human Rights or enforceable EU law.

Justice Minister Paul Maynard said:

It is absolutely right that legal aid should be available to

separated migrant children to resolve their immigration status, which is why this has always been available through the Exceptional Case Funding Scheme.

The changes we are bringing in will mean they can access the support they need quicker and more easily.

The Ministry of Justice has worked with The Children's Society and other children's charities on the amendment and will continue to do so as it comes into force.

Dr. Sam Royston, Policy and Research Director at The Children's Society said:

The Children's Society is pleased the government is moving forward in their promise to reinstate legal aid for thousands of separated and unaccompanied children for all of their immigration and citizenship cases.

Once approved, the changes will make sure this vulnerable group are able to access free advice and representation to resolve immigration issues and secure their citizenship.

It will ensure this can be done without the stress of applying for exceptional case funding, or trying to navigate complex immigration rules and human rights law all alone.

The amendment is in addition to publication of the department's Legal Support Action Plan earlier this year. This committed to improving the Exceptional Case Funding scheme, expanding the scope of legal aid in all Special Guardianship Orders in private family law cases, and will remove the means test for parents or those with parental responsibility who wish to oppose applications for placements or adoption orders.

Reviews have also begun into the legal aid means test to ensure accessibility into the future, along with the entire criminal legal aid system through the Criminal Legal Aid Review.

Jeremy Wright's Oral Statement on the Telecoms Supply Chain Review

Mr Speaker, with permission I would like to make a statement.

New telecoms technologies and next generation networks like 5G and full fibre can change our lives for the better. They can give us the freedom to live and work more freely, they can help rural communities to develop thriving digital economies and help the socially isolated maintain relationships. They can transform manufacturing and make possible connected and autonomous vehicles, smart clothes and agriculture.

But we can only begin this revolution with confidence if our critical infrastructure remains safe and secure.

We know that there are those who have the intention and the capability to carry out espionage, sabotage and destructive cyber attacks against our communications sector.

And the move to 5G brings a new dimension to these risks, given the increased dependence that our national infrastructure is likely to have on those networks over time.

That's why soon after taking up this office I commissioned a review into the UK Telecoms Supply Chain, involving government, industry, international partners and the National Cyber Security Centre, and designed to assess the security and resilience of the UK's telecoms networks, and determine what should be done to improve them.

Today I have published it's conclusions.

The Review identified three key areas of concern.

Firstly, that existing arrangements may have achieved good commercial outcomes but have not incentivised cyber security risk management.

Secondly, that policy and regulation in enforcing telecoms cyber security needs to be significantly strengthened to address these concerns.

And finally, that the lack of diversity across the telecoms supply chain creates the possibility of national dependence on single suppliers, which poses a range of risks to the security and resilience of UK telecoms networks.

The Review has concluded that the current level of protections put in place by industry are unlikely to be adequate to address the identified security risks and deliver the desired security outcomes.

So, to improve cyber security risk management, policy and enforcement, the Review recommends the establishment of a new security framework for the UK

telecoms sector. This will be a much stronger, security based regime than at present.

The foundation for the framework will be a new set of Telecoms Security Requirements for telecoms operators, overseen by Ofcom and government.

These new requirements will be underpinned by a robust legislative framework. We will pursue legislation at the earliest opportunity to provide Ofcom with stronger powers to allow for the effective enforcement of the Telecoms Security Requirements and to establish stronger national security backstop powers for government.

Until the new legislation is put in place, government and Ofcom will work with all telecoms operators to secure adherence to the new requirements on a voluntary basis.

Operators will be required to subject vendors to rigorous oversight through procurement and contract management. This will involve operators requiring all their vendors to adhere to the new Telecoms Security Requirements.

They will also be required to work closely with vendors, supported by government, to ensure effective assurance testing for equipment, systems and software, and to support ongoing verification arrangements.

In addition, we must have a competitive, sustainable and diverse supply chain, if we are to drive innovation and reduce the risk of dependency on individual suppliers.

The Government will therefore pursue a targeted diversification strategy, supporting the growth of new players in the parts of the network that pose security and resilience risks.

We will promote policies that support new entrants and the growth of smaller firms.

This includes research and development support, promoting interoperability and demand stimulation, for example through the Government's 5G Trials and Testbeds Programme.

And we will also seek to attract trusted and established firms to the UK market.

Because a vibrant and diverse telecoms market is not just good news for our consumers, but it is good news for our national security too.

The review also concludes that there should be additional controls on the presence in the supply chain of certain types of vendor which pose significantly greater security and resilience risks to UK telecoms.

The House naturally will be particularly concerned, of course, with the position of the Chinese technology firm Huawei. The government is not yet in a position to decide what involvement Huawei should have in the provision of the UK's 5G network and I want to explain why that is.

On 16th of May the US government added Huawei Technologies Ltd and 68 affiliates to its Entity List on national security grounds.

US companies now have to apply for a licence to export, re-export or transfer a specified range of goods, software and technology to Huawei and named affiliates, with a presumption of denial. On 20th May the US government issued a 90 day Temporary General Licence that authorises transactions in relation to specified areas. These measures could have a potential impact on the future availability and reliability of Huawei's products together with other market impacts and so are relevant considerations in determining Huawei's involvement in the network.

Since the US government's announcement we have sought clarity on the extent and implications but the position is not yet entirely clear. Until it is, we have concluded it would be wrong to make specific decisions in relation to Huawei.

We will do so as soon as possible.

But I also believe Mr Speaker that it would be unnecessary and unwise to delay the introduction of the remainder of the Telecoms Supply Chain Review's Conclusions.

The Telecoms Security Requirements the Review proposes must apply to all companies that want to supply equipment and services in our telecoms supply chain, wherever they come from.

The Review I commissioned was not designed to deal only with one specific company and its conclusions have much wider application.

And the need for them is urgent. The first 5G consumer services are launching this year.

And the equally vital diversification of the supply chain will take time.

We should get on with it.

Mr Speaker, I recognise that colleagues may wish to pursue further the technical detail of the proposals the Telecoms Supply Chain Review makes, not least with officials at the National Cyber Security Centre, who will be available to answer questions in Room 0 from 10.00am to 11.00am tomorrow morning.

But I hope the whole House will agree that the future of our digital economy depends on trust in its safety and security.

And that if we are to encourage the future scale-up of new technologies that will transform our lives for the better, then we need to have the right measures in place to make our telecoms supply chain both safe and secure. That is what the approach proposed in this review will deliver, and I commend it and this statement to the House.

<u>Government plans to safeguard the</u> <u>future security of UK Telecoms</u>

New telecoms security legislation to be introduced and cyber security risks to be prioritised across the sector.

Published 22 July 2019 From: <u>Department for Digital</u>, <u>Culture</u>, <u>Media & Sport</u>, <u>National Cyber Security Centre</u>, and <u>The Rt Hon Jeremy Wright MP</u>



Digital Secretary Jeremy Wright has today set out plans to improve security standards and practices across the UK's telecoms sector, including in new 5G and full fibre broadband networks. The proposals include new legislation to enforce stronger security requirements in the telecoms sector and protect the UK from threats.

The <u>Telecoms Supply Chain Review</u> outlines the Government's ambition to create a sustainable and diverse telecoms supply chain — safeguarding the UK's national security interests and building on our existing capabilities.

At the Supply Chain Review's foundation will be a series of new telecoms security requirements. Overseen by Ofcom and Government, the telecoms operators will need to design and manage their networks to meet these new standards. They will also be subject to rigorous oversight as part of their procurement and contract management processes.

Operators will also need to work much more closely with suppliers to ensure that there is proper assurance testing for equipment, systems and software.

Digital Secretary Jeremy Wright said:

The UK telecoms sector must prioritise secure and safe networks for consumers and business. With the growth of our digital sector and transformative new services over 5G and full fibre broadband in the coming years, this is not something to compromise on. People expect the telecoms sector to be a beacon of safety and this review will make sure that safety and security is at the forefront of future networks.

In response to the Review's findings, the Government will establish a new, robust security framework for the UK telecoms sector — marking a significant shift from the current model.

This new framework will ensure operators build and operate secure and resilient networks, and manage their supply chains accordingly. They will have to assess the risks posed by vendors to network security and resilience, and ensure they manage those risks appropriately.

The Review also identified a lack of diversity in the supply chain and recommends that regulations enforcing telecoms cyber security must be strengthened.

The Government will now develop legislation and look to provide Ofcom with stronger powers. Until then, the government will work with industry to develop new security requirements.

Ciaran Martin, National Cyber Security Centre (NCSC) CEO, said:

As the UK's lead technical authority, we have worked closely with DCMS on this review, providing comprehensive analysis and cyber security advice. These new measures represent a tougher security regime for our telecoms infrastructure, and will lead to higher standards, much greater resilience and incentives for the sector to take cyber security seriously.

This is a significant overhaul of how we do telecoms security, helping to keep the UK the safest place to live and work online by ensuring that cyber security is embedded into future networks from inception.

High risk vendors

The review also looked at how to mitigate the risks from high risk vendors.

The Government continues to consider its position relating to high risk vendors. Following action by the US Department of Commerce and uncertainty around the implications for the telecoms market as a whole from the entity listing, the government is further considering its position relating to high risk vendors. Decisions in this area will be made in due course.

Public consultation on new laws launches to protect armed forces from historical allegations

The Government asks public for views on new measures to ensure military personnel and veterans are not subject to repeated prosecutions

Published 22 July 2019 From: <u>Ministry of Defence</u> and <u>The Rt Hon Penny</u> Mordaunt MP



Defence Secretary Penny Mordaunt has today launched a public consultation on new measures to provide stronger legal protections for serving and former armed forces personnel from alleged historical offences.

In recent years, overseas operations have given rise to thousands of allegations of wrongdoing, most of which only emerged years after the event. These have had a significant impact on members of the armed forces and veterans who have either been the subject of criminal investigations or interviewed as witnesses. At the same time, others have been called upon to give evidence on behalf of the Ministry of Defence, which has had to deal with thousands of civil claims at a great cost to the taxpayer.

The consultation, which will be open for 12 weeks, will allow the public to share their views on new proposals to ensure that service personnel and veterans are not subjected to repeated investigations on historical operations. The proposals include:

• Creating in law a presumption that current or former personnel will not normally face prosecution for alleged offences committed in the course of duty abroad more than 10 years ago

- Creating a new partial defence to murder, which would allow the courts to recognise the operational context in which deaths occur
- Restricting the ability of the Courts to extend the time limit for bringing civil claims for personal injury and/or death

Defence Secretary Penny Mordaunt said:

If we are asking people to put their lives on the line to protect our country, we need to make sure we look after them in return.

The proposed new measures are not about making the armed forces somehow above or exempt from the law, but recognising the unique pressures faced by personnel in the field. They will also ensure that, save for exceptional cases, personnel will no longer have to live with the threat of prosecution hanging over them for many years after the alleged incident.

The consultation proposes legislating for a presumption against prosecution for alleged offences committed on operations abroad over ten years ago because the law currently does not allow for lines to be drawn under allegations with any confidence. Under this proposal, any prosecutions for offences committed over ten years ago would only be taken forward under exceptional circumstances, such as significant new evidence emerging.

It also proposes amending the law to better reflect the operational context, and the unique pressures faced by military personnel — particularly junior soldiers, who may otherwise be prosecuted for murder in relation to deaths where quick decisions were made in highly pressured situations. The proposed partial defence to murder would mean that personnel who cause death by using more force than strictly necessary for self-defence would have their conviction reduced from murder to manslaughter. In these circumstances, the requirement for the initial use of force for self-defence must still be justified.

The third proposal is to change the time limit for civil litigation. Military operations in Iraq resulted in claims being brought against the MOD on an industrial scale, with nearly 1000 claims seeking compensation for personal injury or death. The current law which provides a time limit to such cases — three years for personal injury or death and one year for human rights climates — gives the courts broad discretion to allow claims to proceed, even when they are brought many years after the limit. The MOD's proposals would restrict the court's discretion to extend the time limit to ten years, allowing a line to be drawn under claims for historical incidents overseas.

While the proposals outlined today will provide further protections to UK forces, the military will continue to operate to strict and high standards, complying with both UK and international law, including the Geneva Conventions. Any allegations of wrongdoing will continue to be investigated properly and the armed forces will continue to be held to account.

Today's consultation does not cover Northern Ireland as the MOD is feeding

into the next steps of the Northern Ireland Office's work on addressing legacy issues of Northern Ireland's past. This includes contributing lessons learned from the department's experience of the Iraq Historic Allegations Team and of historical investigations into allegations from Afghanistan.

<u>Lord Ahmad's statement on Tristan da</u> Cunha after severe storms

Tristan da Cunha, a British Overseas Territory in the South Atlantic, has been hit by severe storms this week. The UK Government is working with the local government to help the island get back on its feet.

To help, funding has been principally agreed for emergency repairs. Contractors to help with repairs have been identified and are on standby to travel to the island next week.

Lord (Tariq) Ahmad of Wimbledon, Minister of State for the Overseas Territories, said:

Our quick response to the storms in Tristan de Cunha, which is in the South Atlantic, embodies the broader preparedness work the UK Government is doing to be ready for the 2019 hurricane season in the Caribbean.

Hurricanes Irma and Maria left some Overseas Territories badly affected in 2017. We are working closely with all Territories so they are better prepared for natural disasters before they strike.

To further the UK's quick response to the storms on Tristan, the Foreign Office are looking at options to send an engineer and equipment to the island to restore FCO's satellite link, which provides phone and internet to the whole island.

The Administrator is currently off-Island (in the UK), but is in contact with his team via satellite phone and is making plans to return on the relief ship next week.

The UK's Governor, resident on nearby Overseas Territory St Helena, and the Foreign Office are exploring other options for assistance.

Island representatives have thanked the UK for their quick response.