



House of Lords
House of Commons

Joint Committee on Human Rights

Transnational repression in the UK: Government Response

Sixth Special Report of Session 2024–26

HC 1405

Joint Committee on Human Rights

The Joint Committee on Human Rights is appointed by the House of Lords and the House of Commons to consider matters relating to human rights in the United Kingdom (but excluding consideration of individual cases); proposals for remedial orders, draft remedial orders and remedial orders. The Joint Committee has a maximum of six Members appointed by each House, of whom the quorum for any formal proceedings is two from each House.

Current membership

House of Lords

[Lord Alton of Liverpool](#) (Crossbench; Life peer) (Chair)

[Lord Dholakia](#) (Liberal Democrat; Life peer)

[Baroness Kennedy of The Shaws](#) (Labour; Life peer)

[Baroness Lawrence of Clarendon](#) (Labour; Life peer)

[Lord Murray of Blidworth](#) (Conservative; Life peer)

[Lord Sewell of Sanderstead](#) (Conservative; Life peer)

House of Commons

[Juliet Campbell](#) (Labour; Broxtowe)

[Tom Gordon](#) (Liberal Democrat; Harrogate and Knaresborough)

[Afzal Khan](#) (Labour; Manchester Rusholme)

[Alex Sobel](#) (Labour; Leeds Central and Headingley)

[Peter Swallow](#) (Labour; Bracknell)

[Sir Desmond Swayne](#) (Conservative; New Forest West)

Powers

The Committee has the power to require the submission of written evidence and documents, to examine witnesses, to meet at any time (except when Parliament is prorogued or dissolved), to adjourn from place to place, to appoint specialist advisers, and to make Reports to both Houses. The Lords Committee has power to agree with the Commons in the appointment of a Chairman.

Publication

This Report, was Ordered by the House of Commons, on 22 October 2025, to be printed. It was published on 30 October 2025 by authority of the House of Commons. © Parliamentary Copyright House of Commons 2025.

This publication may be reproduced under the terms of the Open Parliament Licence, which is published at www.parliament.uk/copyright.

Committee reports are published on the Committee's website at www.parliament.uk/jchr and in print by Order of the House.

Contacts

All correspondence should be addressed to the Clerk of the Joint Committee on Human Rights, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 0207 219 2793; the Committee's email address is jchr@parliament.uk. You can follow the Committee on X (formerly Twitter) using [@HumanRightsCtte](https://twitter.com/HumanRightsCtte).

Sixth Special Report

The Joint Committee on Human Rights published its Seventh Report of Session 2024–26, [Transnational repression in the UK](#) (HC 681 / HL Paper 160), on 30 July 2025. The Government response was received on 6 October 2025 and is appended below.

Appendix: Government Response

Introduction

The UK Government is grateful to the Joint Committee on Human Rights (JCHR) for its report on transnational repression (TNR) and its constructive recommendations. This response directly addresses the Committee’s findings and outlines the steps the Government is taking to implement and build upon its recommendations. It complements the Government’s written evidence submission and the oral evidence provided by the Security Minister in May 2025. It outlines the UK’s strategic, legislative, and operational framework for countering TNR, and sets out the steps being taken to strengthen our response.

The UK recognises TNR as a term to describe certain foreign state-directed crimes against individuals. This activity can take place both physically and online, with examples including intimidation, surveillance, harassment, forced/coerced return, abduction, and even assassination at the most serious end of the scale. TNR can undermine an individual’s ability to exercise their freedoms and human rights. However, it is also a matter of national sovereignty and national security.

Since the submission of HMG’s written evidence, and as detailed in the Security Minister’s oral evidence, the Defending Democracy Taskforce (DDTF) has concluded its comprehensive review into TNR. The Review

found that the UK maintains a hard operating environment for those states wishing to conduct TNR and that we have a robust tools and system-wide safeguards in place to counter this threat, including the National Security Act 2023.

The Review made several recommendations to strengthen the UK's response even further, which the Government is actively delivering on, in line with the JCHR's recommendations. These actions include: the introduction of police training; the publication of practical guidance on GOV.UK for individuals who believe they may be at risk; the establishment of a dedicated team within the Home Office to coordinate the UK's strategy on TNR; and the signing of a G7 Leaders' Statement on TNR in June 2025, marking an important milestone in collaboration with international partners.

This Government acknowledges the importance of proportionate, evidence-led responses. Therefore, we continue to engage with law enforcement, civil society, and international partners to refine our approach. The UK's flexible description enables effective collaboration and avoids the limitations of rigid categorisation.

Efforts are underway to further improve data collection and ensure that victims continue to receive appropriate support. International collaboration remains central to the UK's strategy. In addition to the G7 Leaders' Statement, the UK has issued a joint statement in August 2025, alongside G7 Rapid Response Mechanism (RRM) partners, condemning the latest round of arrest warrants and bounties issued by the Hong Kong Police Authorities as acts of TNR. We are supporting the development of the G7 Digital TNR Academy and have launched the Common Good Cyber Fund to assist high-risk individuals. These initiatives reflect the UK's commitment to building collective resilience and raising the cost to perpetrating states to undertake activity amounting to TNR.

In line with the Committee's recommendations, the Government will keep its approach to TNR under regular review. The cornerstone of our approach is the importance of a proportionate and evidence-led response. As the threat evolves, so too will our response - ensuring that our systems are constantly improving to remain effective at protecting individuals and communities and aligned with the UK's broader national security and democratic resilience objectives.

Recommendations

Definition and Legal Framework

Recommendation 1 (Paragraph 21): We recommend that the Government adopt a formal definition of transnational repression. This should be developed in consultation with law enforcement, civil society and affected communities. It should include, as core elements, the ‘involvement’ of a foreign state, and the targeting of individuals located outside that state’s jurisdiction. The definition should be sufficiently broad to encompass victims of TNR regardless of their ethnicity or nationality. In addition to adopting a legal definition, authorities should be equipped with clear guidance and explanatory materials outlining the various forms transnational repression can take.

Response:

1. TNR is a matter of national security and national sovereignty, but also about undermining an individual’s ability to exercise their rights and freedoms. The UK recognises TNR as a term to describe certain foreign state-directed crimes against individuals. This activity can take place both physically and online, with examples including intimidation, surveillance, harassment, forced/coerced return, abduction and even assassination at the most serious end of the scale.
2. The Government accepts the Committee’s view that any definition should be sufficiently broad to capture the full range of victims. We agree with this principle and have intentionally shaped our description to reflect this. The Government’s description of TNR was developed through the Defending Democracy Taskforce’s Review and informed by engagement with law enforcement, civil society, and affected individuals. It ensures that all victims are recognised, regardless of ethnicity or nationality, and avoids introducing limitations based on community affiliation or motivation, which are often difficult to conclusively establish. This approach provides maximum flexibility to respond to the evolving threat and aligns as closely as possible with international partners’ interpretations.
3. The Government’s description of TNR captures the totality of the issue and the full spectrum of threats - from online harassment to assassination at the most serious end of the scale. TNR is not a new phenomenon and the UK’s legal, policy and operational responses to this type of harm have developed over decades. The National Security Act 2023 provides a comprehensive suite of powers to tackle TNR, in particular, the Foreign Interference Offence and the state threats aggravating factor, which enable conduct to be prosecuted where it is carried out for or on behalf of a foreign

power. Therefore, the Government agrees with the Committee's conclusion that the creation of additional criminal offences is not necessary at this time to address the challenges posed by TNR.

4. Our approach is designed to encourage reporting and ensure that victims receive the support and protection they need. Law enforcement agencies are already receiving training on state threats and foreign interference, including how to identify and respond to activity that may amount to TNR. This training is available to all police forces and is being rolled out alongside a programme of briefings and awareness-raising.
5. While there is no universally agreed international definition of TNR, the UK's flexible approach enables effective collaboration with likeminded partners. The Government want individuals to feel confident reporting any incident of state-directed crime, without needing to consider whether or not their experience meets a strict definition.
6. The Government will continue to keep its approach under review, including the potential utility of further explanatory materials or guidance, to ensure that all relevant bodies are aligned in their understanding of what constitutes TNR and that there are appropriate mechanisms in place for addressing it. We remain open to considering further steps that support clarity and coordination, in line with the Committee's emphasis on ensuring a joined-up response.

Recommendation 2 (Paragraph 22): Without clear data on the scale and nature of TNR events in the UK, it is difficult both to create effective policy responses and to judge the effectiveness of the Government's new TNR strategy. The Government should ask police forces to collect relevant data on the number and nature of TNR reports in the UK. This data should then be used to review the effectiveness of the new TNR strategy and to identify countries of concern. This approach will enhance the UK's capacity to identify patterns of state-linked harassment and coercion, and to respond more effectively to the evolving threat landscape. We recommend that, in cases where reports of TNR do not lead to prosecution or further action, law enforcement agencies should nonetheless record and retain relevant data, where appropriate, to support TNR trend analysis and future investigative efforts.

Response:

1. The Government recognises the importance of robust data and evidence in shaping an effective response to transnational repression (TNR). We are taking active steps to strengthen our understanding of the threat, improve data collection, and ensure that our systems are responsive and proportionate.
2. A key focus of the Defending Democracy Taskforce's Review was to understand the scale and nature of TNR in the UK. This included identifying methodologies and patterns of behaviour associated with TNR to ensure that our response is robust and that sufficient safeguards and mitigations are in place to prevent such activity from occurring.
3. The Review found that TNR tends to be targeted and specific, with perpetrating states focusing on individuals they perceive as threats - such as vocal critics, dissidents or activists. While TNR does not therefore affect large numbers of people across the UK, its impacts can be severe, both for the individuals directly targeted but also for wider communities, where fear and concern may spread. This can create a "chilling effect," which can lead individuals to self-censor and the gradual curtailment of democratic freedoms, such as attending protests or political/cultural events. It is therefore essential that our response remains proportionate, protective and adaptable, regardless of the scale of the problem.
4. We continually assess potential threats in the UK and draw on a multisource model to build a comprehensive picture of that threat. This includes intelligence assessments, engagement with international partners, and insights from civil society and affected individuals.
5. This Government works closely with law enforcement and other partners to continue to strengthen our understanding of reporting trends and methodologies. This includes identifying patterns of behaviour and ensuring that sufficient safeguards and mitigations are in place to prevent TNR from occurring. A dedicated team has now been established within the Home Office to coordinate this work and act as a focal point across HMG.
6. To further support data collection, policing has established a system for the reporting of crimes that includes reference to foreign interference, where these should be logged, then reviewed and actioned by specialist teams accordingly. The collection and aggregation of data is part of this developing process and will assist policing and the Government in developing a more detailed understanding of reported activity across the country, including activities and reporting countries of concern. This will assist in the development and review of strategy and interventions. This evolving approach aligns with the Committee's recommendation to strengthen data collection and analysis.

7. The Government recognises that external sources, including academic and NGO reporting, can provide valuable insights. However, attribution to foreign states – who often deploy sophisticated tradecraft to avoid detection- is inherently complex, and care must be taken to ensure that policy is informed by robust, verifiable data. Our approach is to build a clear and accurate picture of the threat landscape, while avoiding the risks of spurious or misattributed claims shaping operational or strategic decisions.
8. The Government will continue to develop its understanding of TNR and ensure that the systems in place to detect, deter and counter this activity remain effective and proportionate.

Recommendation 3 (Paragraph 27): However, we recognise the rapidly evolving nature of digital technologies and the increasing sophistication of methods used to conduct TNR. It is therefore essential that the legal framework remains agile and responsive to evolving threats. We recommend that the Government keeps relevant legislation under regular review to ensure it remains fit for purpose in addressing emerging threats, particularly those facilitated by advances in artificial intelligence and surveillance capabilities. The Government should write to this Committee annually to provide an update on the effectiveness of current legislation at addressing evolving digital forms of TNR.

Response:

1. We are pleased that the Committee recognises the effectiveness of the National Security Act 2023 in relation to TNR. This new legislation was designed with modern day state threats in mind and constructed to be future proofed as well as having extraterritorial reach. In Part 3 of the Act, there is a statutory requirement for the operation of Parts 1 and 2 of the Act, which include the provisions relevant to TNR, to remain under review by the Independent Reviewer of State Threats Legislation. As part of this requirement, the Home Secretary must lay before Parliament a report from the Independent Reviewer detailing the outcome of their annual review. As such, any inadequacies in the legislation to deal with threats such as those posed by digital forms of TNR are expected to be identified through this existing reporting function.
2. Whilst the heart of the UK's legislative framework for deterring and combatting activity that amounts to, or is akin to, transnational repression, is the National Security Act 2023, there is other domestic legislation complementary to these aims. This includes the Online Safety Act, which enhances the regulation of online platforms, ensuring the safety of users. The Act imposes duties on platforms to tackle the spread of illegal content, particularly content amounting to one of the priority offences in the Act. This includes the Foreign Interference Offence, requiring platforms to take

proactive measures to tackle illegal attempts by (or on behalf of) foreign powers to interfere in UK interests on their services. The Government is closely monitoring the implementation and effectiveness of the Act and remains committed to strengthening our laws if it does not deliver the necessary protection to ensure a safer online environment.

3. The Defending Democracy Taskforce's Review highlighted the evolving nature of the threat, including the increasing use of digital platforms and emerging technologies. It also emphasised the importance of identifying methodologies and patterns of behaviour to ensure that our response remains robust, and that sufficient safeguards and mitigations are in place to prevent TNR.
4. Emerging technologies, including artificial intelligence, present both risks and opportunities in this context. Malign actors may use these tools to scale harassment or disinformation campaigns, but they also offer new capabilities to detect and disrupt such activity. The UK is actively exploring these opportunities through initiatives such as the Common Good Cyber Fund, which supports specialist nonprofit cybersecurity organisations to deliver defensive solutions to high-risk individuals and groups.
5. Ultimately, legislation alone will not address the full spectrum of TNR threats. The Government is committed to a whole-of-system response, combining legal powers with operational tools, international collaboration, and targeted engagement with civil society and affected communities.

Recommendation 4 (Paragraph 33): The Government should ensure that TNR is a high priority consideration when deciding which countries should be specified under the enhanced tier of the Foreign Influence Registration Scheme. Decisions on which countries to specify under the enhanced tier of FIRS must be guided by objective assessments of threat, not influenced by broader foreign policy considerations. We recommend that the Government specify China under the enhanced tier of FIRS. China conducts the most comprehensive TNR campaign of any foreign state operating in the UK. Its omission from the enhanced tier risks undermining the credibility and coherence of FIRS. Any attempt to specify only isolated parts of the Chinese state in the FIRS would fail to reflect the true nature and complexity of the threat, as influence operations span all sectors of the economy and lack clear command-and-control structures.

Response:

1. FIRS imposes registration requirements on certain activity in the UK that is directed by foreign powers or entities. The political tier provides transparency to those who may be seeking to carry out political influence activity on behalf of a foreign state.
2. The enhanced tier provides greater assurance around the activities of the foreign powers or entities which pose the greatest risk to the UK. It requires those acting in the UK at the direction of a specified foreign power or foreign power-controlled entity to register. It also requires specified foreign power-controlled entities to register activities that they carry out themselves in the UK. The activities requiring registration under the enhanced tier could include activities which may repress individuals perceived to be a threat. The Government recognises that activity amounting to transnational repression is relevant to this assessment and will ensure it is considered in decisions regarding specification under the enhanced tier.
3. The Secretary of State may specify a country or part of a country under the enhanced tier where they consider specification to be reasonably necessary to protect the safety or interests of the UK. This requires the consideration of a broad range of interests, including but not limited to, security considerations. As with all risks to the UK's national security, the risk posed by TNR will be carefully considered as part of this process, in agreement with the Committee's recommendation. We will continue to keep specifications on the enhanced tier under constant review to ensure we are protecting the safety and interests of the UK. Countries are considered separately for specification and any changes to the countries listed will be announced first in Parliament in the usual way. No decision has been taken on whether we should specify China on the enhanced tier of the scheme. The implementation of the political tier of the scheme on 1 July ensures that any foreign influence in our democracy, including from China, needs to be declared. This is a significant step forward in protecting our democracy from interference.

Recommendation 5 (Paragraph 34): The Home Office and relevant enforcement bodies should develop clear guidance on how FIRS data can be used to support investigations into TNR, and regular reviews should be conducted to assess the scheme's effectiveness in this regard.

Response:

1. The Home Office worked closely with law enforcement partners to prepare for the scheme and clear processes are in place to ensure compliance. The objectives of FIRS are to encourage transparency, deter harmful covert state threat activity and increase the opportunity for earlier disruptions. The

Government will monitor progress against these objectives, and will also consider the scheme's impact in a range of scenarios including responding to activity that constitutes TNR.

2. Additionally, the Government will publish an annual report which will, among other things, make clear the number of registrations under the scheme and the number of persons charged and convicted of offences of non-compliance.

Recommendation 6 (Paragraph 41): In response to this report, the Government should provide this Committee with a clear timeline in which it plans to review the effectiveness of the SLAPPs provisions in the Economic Crime and Corporate Transparency Act 2023. The Government should also set out the criteria it intends to use to assess whether these provisions have worked as intended. The Government should use the results of this review to inform the drafting of future legislation to address SLAPPs that are not related to economic crime.

Response:

1. The Government commenced sections 194 and 195 of the Economic Crime and Corporate Transparency Act 2023 (ECCTA) on 18 June 2025, which are designed to tackle Strategic Litigation Against Public Participation (SLAPPs) claims related to economic crime. This marks a significant first step in addressing this abusive practice, which employs intimidation tactics to silence individuals exercising their right to free speech on matters of public interest.
2. The Government understands the profound financial and psychological impact SLAPPs have on victims, and their effect on our legal system and society. They curtail free speech, have a chilling effect on public interest journalism and pose a threat to our democracy.
3. The Civil Procedure Rule Committee (CPRC) approved amendments to the Civil Procedure Rules to fulfil the requirement under section 194 of the ECCTA, introducing a bespoke early dismissal mechanism for SLAPPs that lack sufficient merit. These amendments also provide costs protection for defendants in cases that proceed to trial. In addition, section 195 of ECCTA establishes a statutory definition of economic crime-related SLAPPs.
4. While this is a positive first step, it is important to clarify that the Government is considering its future approach to comprehensively addressing all SLAPPs - not just those related to economic crime. This future strategy will be informed by insights gained from the operation of the ECCTA.

5. The Government has committed to monitoring the procedural rules and will report back to CPRC one year after implementation, by June 2026. The timing of any such review, however, shall remain contingent upon case volumes. The Government is currently finalising the criteria for assessing the effectiveness of the ECCTA provisions and will update this Committee at an appropriate juncture.

Policing and Support for Victims

Recommendation 7 (Paragraph 45): We recommend that the Government develop and implement a proactive outreach strategy aimed at individuals and communities likely to be at high risk of TNR. This strategy should be developed within 12 months and include clear timelines for how engagement activities will be rolled out. The Government should engage with diaspora groups, civil society organisations, and community leaders to provide practical guidance on the methods and tactics commonly used in TNR, as well as the steps individuals can take to enhance their personal safety and access appropriate support and reporting mechanisms.

Response:

1. As noted in the response to **Recommendation 2**, TNR in the UK tends to be targeted and specific. While TNR does not affect large numbers of people across the UK, its impacts can be severe - not only for those directly targeted but also for wider communities, where fear and concern may spread.
2. It is therefore critical that the Government's response is proportionate and effective - reassuring individuals that they can exercise their democratic rights freely and with confidence, without inadvertently creating a climate of fear. Our approach is guided by the principle of "be alert but not afraid". We do not refer to entire communities as "high risk", nor do we seek to profile or expose groups to unnecessary scrutiny. Doing so risks alienating individuals, dividing communities, and inadvertently achieving the objectives of authoritarian states.
3. Nuanced threats, such as TNR, are inherently difficult to communicate and can be misinterpreted or manipulated. We are mindful of the risks posed by misinformation and false accusations, and we take care to ensure that our public messaging does not contribute to panic or confusion. Furthermore, as noted in our written evidence, communities are not monolithic - they are made up of a range of individuals with differing experiences and backgrounds, so it is essential to qualify the use of these terms with nuance and context. For these reasons, community engagement initiatives - run

by local authorities and central government departments - focus on integration and resilience, helping individuals feel part of UK society and confident in their rights and freedoms.

4. The Government recognises the importance of proactive engagement and continues to undertake targeted outreach with civil society organisations, think tanks, and NGOs, including those advocating on behalf of individuals affected by TNR. Officials engaged with victims, community leaders and academics during the Defending Democracy Taskforce's TNR Review, and this engagement has and will continue at both Ministerial and official levels. We will factor the Committee's recommendation into the development of future engagement activity.
5. The Government has also published practical guidance on GOV.UK for individuals who believe they may be at risk of TNR. This guidance offers advice on both physical and online safety, signposts reporting mechanisms, and links to wider protective security resources. It is designed to be accessible and proportionate - providing reassurance without exacerbating fear.
6. In addition, as mentioned in the response to **Recommendation 1**, law enforcement agencies are receiving training on state threats and foreign interference, including how to identify and respond to activity that may amount to TNR. This training is available to all police forces and is being rolled out alongside a programme of briefings and awareness-raising. This ensures that frontline officers are equipped to respond appropriately and sensitively to reports from individuals who may be at risk.
7. Overall, the UK Government has developed a range of support and security assistance mechanisms to protect individuals who may be at risk of TNR. This assistance is based on threat and varies in scope and approach, but can include tailored protective advice, cybersecurity measures, and access to broader public resources. For security reasons, it would not be appropriate to comment on the specifics of these arrangements. We remain committed to refining our approach and will take the Committee's recommendation into account as part of ongoing work to strengthen outreach and support.

Recommendation 8 (Paragraph 49): We recommend that the content of this guidance be reviewed regularly, with input from victims, to ensure it is genuinely effective and helpful for victims and that it remains responsive to evolving TNR tactics. The Government should ensure that this guidance is made available in multiple languages within six months, this should include languages commonly spoken by affected communities. We further recommend that the Government take proactive steps to promote this existence of this guidance amongst communities at high risk of experiencing TNR.

Response:

1. The Government welcomes the Committee's recognition of the online [guidance](#) published on 14 May for individuals who believe they may be at risk of TNR. This guidance is a key part of our broader effort to ensure that victims and at-risk individuals have access to clear, practical advice on how to protect themselves and report concerns. We agree that ensuring this guidance remains visible, relevant and accessible is essential.
2. The guidance is designed to be accessible and practical, offering advice on both physical and online safety. It is integrated with wider protective security resources, including those from the National Cyber Security Centre and the National Protective Security Authority, and supports existing reporting mechanisms, including how to contact the police and what to expect when doing so.
3. The Government agrees that this guidance must remain responsive to the evolving nature of TNR. To that end, the content will be kept under regular review, informed by operational insights and ongoing engagement with civil society organisations and trusted networks.
4. While the Government does not currently plan to publish the guidance in multiple languages, we remain committed to ensuring it is accessible. Translating and maintaining accurate versions in multiple languages would not be proportionate or beneficial and usage is likely to be low given the targeted and specific nature of TNR in the UK. Prioritising specific languages could risk stigmatising certain communities or inadvertently suggesting that entire groups are under threat or surveillance.
5. Our approach is guided by the principle of "be alert but not afraid". Our engagement is designed to be proportionate, protective, and sensitive to the risks of misinterpretation or misuse. The targeted and specific nature of the threat means victims of TNR benefit most from trusted, personalised engagement, and we continue to work with civil society organisations and professional bodies to disseminate guidance through appropriate channels.
6. The Government will continue to assess the effectiveness and reach of this guidance and remains open to feedback and further enhancements where they would demonstrably and proportionately improve accessibility and impact. We are grateful for the Committee's suggestions, which will inform our ongoing work in this area.

Recommendation 9 (Paragraph 56): The Government should regularly evaluate the uptake of the new police training on transnational repression. Updates on participation rates should be provided to the Committee every six months. If uptake remains limited, serious consideration should be given to making this training mandatory for

all police officers. Police should also be given training on early warning signs of TNR-related risks, such as intimidation of friends and family members abroad.

Response:

- 1.** Policing provides the Government with updates on the delivery of awareness and guidance for forces on a quarterly basis. This focuses on the number of officers and staff who complete online modules on the National Security Act, foreign interference awareness, and security.
- 2.** As noted to the Committee, the Foreign Interference module and operational security modules, which were launched in July 2024, are currently being reviewed and updated, and revised versions are expected to be issued later in 2025. These modules will continue to highlight areas of potential foreign interference and ask officers and staff, including 999 call handlers, to raise any case which may include foreign interference to specialists for assessment. In addition to the online learning, Counter Terrorism Policing (CTP) delivers face-to-face briefings and provides bespoke support for key groups in forces across England and Wales.
- 3.** This training is mandatory for all CTP officers as they are responsible for investigating state threat incidents. CTP notes the Committee's recommendation that making the modules mandatory across policing is kept under consideration and CTP will keep this under review and continue to engage with wider policing on this important issue.
- 4.** At present, the Government considers the current approach to be proportionate. Our response is designed to be adaptable and threat-led, ensuring that officers most likely to encounter TNR-related activity are equipped with the necessary tools and awareness. We remain committed to ensuring that police officers are able to identify and respond to early warning signs of state-directed activity.

Recommendation 10 (Paragraph 62): We recommend that the Government establish a dedicated national reporting hotline for individuals who experience TNR to enhance victim support, improve data collection, and facilitate timely referrals to the appropriate personnel. The reporting hotline should be established within one year of the publication of this report. It should be staffed by personnel specifically trained to identify and respond to TNR, with a clear understanding of the tactics employed by particular state actors and established referral pathways to the appropriate law enforcement agencies. The service should be supported by a multilingual provision, including translated materials and guidance, as well as access to interpreters who can assist callers in their preferred language.

Response:

1. The Government is committed to ensuring that individuals who believe they may be victims of TNR have access to clear, trusted, and effective mechanisms for reporting concerns and receiving support. The Defending Democracy Taskforce's Review carefully considered, in consultation with CTP, how best to encourage reporting and ensure that reports are treated seriously and dealt with appropriately.
2. CTP keep the means and mechanisms for engaging and building community confidence and effective police response under continuous review. As discussed with the Committee, CTP's assessment, developed in conjunction with the Government, is that the 999 and 101 lines are the most widely known and easily accessible means of contacting policing, ensuring that handlers can assess and provide the most appropriate level of assistance, which, when required, can be immediate. This also allows calls to be assessed and referred for further action to specialists depending on the nature of the crime – which includes state threats.
3. Existing police hotlines and reporting mechanisms also include provisions to access translators to assist callers who may not be able to communicate in English, and CTP's work to increase awareness and confidence in reporting across policing includes outreach to and through translation services. CTP is also seeking to increase understanding of TNR among those providing translation services for policing.
4. CTP continue to work with call handlers across policing to ensure that all reports potentially including state threats are flagged to specialist teams for assessment, while also ensuring the local force takes immediate action if and where required.
5. CTP believes that introducing a bespoke reporting hotline for TNR would be duplicative and potentially cause confusion. There is a risk it might be unclear what number individuals should call and when, and such a system could undermine the clarity and effectiveness of existing mechanisms. Given the targeted and specific nature of TNR in the UK, expected call volumes would be low, and the resource investment required to establish and maintain a separate hotline would not be proportionate.
6. Moreover, a dedicated hotline risks reinforcing the perception that TNR is widespread or ubiquitous, which could inadvertently spread fear, encourage false reporting, or be misused as a surveillance tool. Our public messaging is designed to be proportionate and protective, and our reporting systems are structured to ensure that police - not the public - triage cases and assess threat levels.

7. The Government will continue to work with policing to strengthen awareness, confidence, and capability in responding to TNR, while ensuring that our approach remains proportionate, effective, and focused on protecting those most at risk.

Recommendation 11 (Paragraph 63): We further recommend that data collected through the hotline be anonymised and recorded to inform policy development and threat assessments.

Response:

1. As referenced in our response to **Recommendation 9**, Policing is building increased systems to collate and analyse data from public reporting to inform the strategic and operational response, policy development and threat assessments.

INTERPOL and visa applications

Recommendation 12 (Paragraph 72): We recommend the Government works with ‘Five Eyes’ and other partners to track and expose malicious, vexatious, and politically motivated use of Red Notices by member states. In doing so, the Government should advocate for greater transparency and accountability within INTERPOL’s procedures and advocate for the use of corrective measures and suspensions for systematic abusers of INTERPOL mechanisms.

Response:

1. INTERPOL is key for sharing information for law enforcement purposes with our European, Five Eyes and other international counterparts. There are rigorous processes put in place by INTERPOL to ensure that Notices and Diffusions are issued in line with the INTERPOL Constitution and INTERPOL Rules of Processing Data. The UK works with colleagues across the INTERPOL membership and with INTERPOL to reinforce this work, particularly in upholding Article 3 of the Constitution, which prohibits using the INTERPOL systems for political, military, religious, or racial ends.
2. We are aware of the potential for the misuse of INTERPOL Red Notices, and other international routes, to have arrest warrants actioned. The Home Office continues to work with the National Crime Agency, which acts as the UK’s National Central Bureau for INTERPOL, to monitor the effectiveness of existing safeguards. If we were made aware of confirmed cases of INTERPOL misuse, we would not hesitate to raise it with INTERPOL’s leadership.

3. Every Red Notice is checked for compliance by the INTERPOL Notices and Diffusions Task Force (NDTF) before issuance, at which point any Notices which are non-compliant are removed. After Notices or Diffusions have been published, the Commission for the Control of INTERPOL's Files (CCF) has the power to investigate, and/or remove, any that can be proved to be in breach of the INTERPOL Constitution. INTERPOL also has the power to impose corrective measures on States found to be misusing INTERPOL systems; whilst it does not make public where these measures have been imposed, all member countries receive regular updates on the corrective measures imposed. As INTERPOL stated in its [written evidence](#) to the Committee, the corrective measures may range from enhanced monitoring of outgoing communication from the country concerned to full disconnection from the INTERPOL Information System.
4. The Government continues to be a strong advocate in support of INTERPOL and its reform programme to ensure there is no space for States to wilfully misuse its systems. We have welcomed the decision by INTERPOL to publish information on the work of the NDTF, specifically the number of Notices and Diffusions published, alongside the number refused by the NDTF: [Compliance and Review](#). The latest statistics highlight that whilst there is, as noted, the potential for misuse of INTERPOL systems, the numbers of Notices and Diffusions identified as in breach of the Constitution represent a small percentage of the overall number eventually published: [About Notices](#). That said, the Government views any allegation of misuse of INTERPOL's systems very seriously and can confirm that we will continue to work closely with INTERPOL and partners to ensure the legitimacy of the Notices and Diffusions system, including through discussions at INTERPOL's Governance Committee, and at meetings of the rules of data processing group.

Recommendation 13 (Paragraph 74): While the option exists for individuals to request access to or removal of their data via INTERPOL's independent oversight body, the Commission for the Control of INTERPOL's Files, this process is often significantly delayed and may not offer timely protection to those at immediate risk. The Government should undertake a review of existing procedures to consider whether it is possible to introduce a formal mechanism by which the Home Office or the National Crime Agency (NCA) may alert individuals of the existence of a Red Notice or Diffusion where there is a strong basis to believe it has been politically motivated

Response:

1. As the Committee's report notes, individuals can already request access to, or removal of, their data via INTERPOL's independent oversight body – the Commission for the Control of INTERPOL's Files (CCF) – which ensures compliance with data rules and resolves disputes as to the legitimacy of Notices or Diffusions. This service is freely available on INTERPOL's website. It would not be appropriate for the UK, or any member State, to check on behalf of individuals, or inform individuals, as to whether they are wanted by other States, as we cannot intervene in the judicial process of other sovereign nations. Therefore, it is right that this process is carried out via the CCF. However, if we were made aware of confirmed cases of INTERPOL misuse, we would not hesitate to raise it with INTERPOL. INTERPOL's Constitution, in particular Article 3 forbids the Organisation from undertaking any intervention or activities of a political, military, religious or racial character. Therefore, if there was a strong basis to indicate a notice was politically motivated, it would not be issued by the Notices and Diffusions Taskforce (NDTF). If an INTERPOL Member Country does not fulfil its obligations under the present rules, the General Secretariat is entitled to take corrective action, as outlined in Article 131 of the INTERPOL Rules on the Processing of Data. Further information on the screening and review process at NDTF is available on their website.

Recommendation 14 (Paragraph 75): In addition, the Government should take proactive steps to protect individuals facing an extradition risk due to a politically motivated Red Notice. A voluntary mechanism should be introduced to allow targeted British Nationals to notify the Foreign, Commonwealth and Development Office (FCDO) of planned travel to high-risk countries. This would give UK missions advance notice and allow them to prepare for early intervention if needed.

Response:

1. There are rigorous processes put in place by INTERPOL to ensure that Notices and Diffusions are in line with the INTERPOL Constitution and INTERPOL Rules of Processing Data. The UK works with colleagues across the INTERPOL membership and with INTERPOL to reinforce this work, particularly in upholding Article 3 of the Constitution, which prohibits the use of Notices and Diffusions for political, military, religious, or racial ends.
2. The decision on whether to travel internationally is one for individuals to take. Local authorities will always be primarily responsible for the safety and security of people in their jurisdiction. Consular assistance to British

nationals is available 24/7 via Foreign, Commonwealth and Development Office (FCDO) contact centres, and the nature of that support is set out in the published guidance [here](#).

3. The FCDO's Travel Advice remains under constant review to ensure it reflects the latest assessment of the risks to British nationals travelling overseas, including to countries of a second nationality.
4. The UK Government recognises that some foreign States may target those whom they perceive to be a threat or otherwise wish to control when travelling overseas. To support those travelling overseas, we have issued personal and cyber guidance on the transnational repression [GOV.UK page for individuals to consider](#).

Recommendation 15 (Paragraph 79): The Home Office should ensure that all relevant immigration staff are adequately trained and informed about the potential misuse of Red Notices. In addition, the Country Policy and Information Notes used in assessing asylum claims should be revised to explicitly address the threat of transnational repression. The Government should update the Committee within six months, outlining what specific steps it has taken to improve training for Home Office staff around politically motivated Red Notices

Response:

5. The Government recognises the importance of ensuring that immigration decision makers are equipped to understand and respond to cases where Red Notices are a consideration. Relevant decision makers in the immigration context already receive extensive guidance around the handling of INTERPOL Red Notices and the processes that need to be followed in a variety of situations. These processes are kept under review.
6. The Country Policy and Information Notes (CPINs) produced by the Home Office aim to cover the main issues arising in protection claims in the UK, which can include TNR. CPINs describe country conditions and do not cover Red Notices as these are case-specific. The assessments in CPINs are based on a careful analysis of available country of origin information – obtained from a range of sources including media outlets; local, national and international organisations; and the FCDO – and take into account relevant asylum policies and refugee law. The Home Office considers what information to include in CPINs in line with its research methodology, which is detailed in each CPIN. These assessments are subject to a rigorous quality control process, including scrutiny from government lawyers and input from external stakeholders, to ensure they are accurate, reasonable, balanced and lawful.

7. All decision makers must consider all claims on an individual basis, taking into account each case's specific facts. In line with the Home Office's responsibility to present a reliable and accurate representation of a situation in a country, any relevant information regarding a particular issue may be considered or included in CPINs where it contributes to the overall assessment of risk.

Departmental Coordination and Diplomatic Policy

Recommendation 16 (Paragraph 87): We recommend that the Government explicitly incorporate transnational repression into the UK's human rights reporting frameworks. In particular, references to TNR should be included in the next iterations of the Foreign, Commonwealth and Development Office's annual Human Rights and Democracy Report and in the Overseas Security and Justice Assistance Guidance. The UK should also ensure that diplomatic responses, such as the expulsion of officials, public demarches, and the imposition of sanctions, are not only available in principle but are actively and visibly deployed in response to serious incidents.

Response:

1. The UK Government's response to TNR recognises this activity is a threat to national security, human rights and democracy, which undermines the rule of law and sovereignty. When alerted to instances of TNR, the FCDO deploys the most appropriate diplomatic measures, both publicly and privately, to raise the cost to foreign states of carrying out interference activity and protect individuals at risk in the UK.
2. We have deployed a range of diplomatic measures to respond to this threat, as outlined in our response, including issuing international statements with likeminded partners, and utilising sanctions to support our response to this activity, further detail is included in the response to **Recommendations 19-21**.
3. The Government takes the protection of individuals' rights in the UK very seriously and is also firmly committed to furthering human rights around the world. We do this by investing in building partnerships, including with civil society, and by drawing on our diplomatic and development levers to deliver meaningful change on the ground.
4. The Annual Human Rights and Democracy Report series demonstrates the UK's long-standing commitment to human rights and has previously included TNR. This Government has decided to refresh and streamline the

format of the Report, spotlighting a small number of topics to showcase the FCDO's delivery on human rights; we will consider including TNR in a future report.

5. The Overseas Security and Justice Assistance (OSJA) framework is HMG's tool for assessing the human rights and International Humanitarian Law (IHL) risks of our overseas security and justice assistance work and identifying measures to mitigate such risks. The FCDO is currently reviewing the OSJA guidance so that it remains fit for purpose and captures emerging risks that could contribute to violations of human rights and IHL. As part of this review, we will consider the Committee's recommendation to reference TNR in the guidance.

Recommendation 17 (Paragraph 89): The Committee recommends that the Government review the scope of the UK's sanctions framework to assess the feasibility of introducing specific TNR sanctions. The UK should also adopt a more proactive approach to sanctions, particularly in cases where UK nationals and residents are directly affected. This should include the timely designation of perpetrators and state actors responsible for systematic TNR in appropriate cases, even in the absence of prior action by international partners

Response:

1. The Sanctions and Anti-Money Laundering Act 2018 (SAML A) gives the government independent powers to impose, implement, enforce and lift sanctions. SAML A has been updated several times to strengthen the sanctions framework, close loopholes and make the system more agile to meet evolving geopolitical challenges.
2. The UK currently has 36 live sanctions regimes. These regimes are sets of sanctions measures focussed on specific countries or policy objectives, designed to achieve defined purposes and enshrined in legislation.
3. In agreement with the principles of the Committee's recommendation, the Government keeps sanctions powers, regimes, designations and measures under review to respond to new developments and changing circumstances. The newest sanctions regime, the Global Irregular Migration and Trafficking in Persons Sanctions Regulations 2025, was laid in Parliament on 22 July.
4. In certain circumstances, the UK can impose sanctions as part of its response to state-directed crimes, including activity amounting to TNR.
5. For example, in April 2025, the UK sanctioned the Iranian-backed Foxtrot criminal network and its leader, Rawa Majid, for their role in attacks against targets across Europe. In January 2024, the UK sanctioned those responsible in the Iranian Revolutionary Guard Corps, along with the

Zindashti Cartel, who are employed by Iran's intelligence services to do its bidding overseas, for their involvement in plots to kill opponents of the regime in the UK and abroad.

Recommendation 18 (Paragraph 90): Due to the national security sensitivities and the need for swift action, there are limited opportunities for Parliament to scrutinise sanctions policy. We recommend that the Government provide regular confidential updates to the Intelligence and Security Committee, outlining the rationale for imposing, or not imposing sanctions, in relevant cases.

Response:

1. Sanctions are carefully designed and targeted. The Government considers the potential domestic and wider impacts, including on the UK economy as well as on the intended target, and considers how such impacts can be mitigated. UK courts have consistently recognised the Government's expertise on matters of foreign policy, including how sanctions can be used to maximum effect.
2. New sanctions regulations go through extensive parliamentary scrutiny. All secondary legislation is subject to high levels of scrutiny by the Secondary Legislation Scrutiny Committee (SLSC) and the Joint Committee on Statutory Instruments (JCSI) or by parliamentarians following the laying of the SI.
3. New autonomous regulations (to amend existing sanctions regimes or introduce new autonomous sanctions regimes) are made under the made affirmative procedure. New UN or mixed UN-autonomous regulations are subject to the made negative parliamentary procedure. This means that MPs and Peers can pass a prayer motion within 40 days of laying to defeat the legislation – though to date this has never happened for sanctions regulations.
4. Designations are developed and deployed by FCDO Ministers using the criteria and legal tests set out in sanctions regulations and the Human Rights Act 1998, all of which have been scrutinised and approved by Parliament.
5. Each designation is subject to ministerial consideration and must adhere to robust legal requirements. The reasoning behind each designation must be properly evidenced according to criteria approved by Parliament, and with credible sources that can be relied upon in court.
6. The Sanctions and Anti-Money Laundering Act 2018 (SAML A) provides the legal framework for designations. Ministers are under a duty to revoke a designation where the relevant tests are no longer met, and designated persons may request a review of their designation; the outcome of that

review can be considered by the courts. Further, a Minister may decide to review a designation at any time - for example, if new information becomes available

7. This Government has proactively updated Parliament in respect of all key sanctions decisions, including via regular oral and written statements, providing opportunities for discussion and challenge.

Recommendation 19 (Paragraph 92): The UK should support efforts to elevate TNR as a priority on the UN agenda and promote coordinated international action against its use by authoritarian regimes. The Government should also ensure that information and data on TNR is shared with likeminded countries through fora such as the Council of Europe, INTERPOL, the G7 Rapid Response Mechanism, OSCE and UN, to help combat TNR at a global level.

Recommendation 20 (Paragraph 93): We recommend that the Government work closely with Canada to strengthen international collaboration on countering TNR during Canada's 2025 G7 Presidency. As part of this effort, the UK should play a leading role in the launch and development of the proposed Digital TNR Detection Academy under the G7 Rapid Response Mechanism. This initiative will enhance collective capacity to detect and respond to online forms of TNR by equipping G7 members and partners with the technical skills and tools needed to identify and counter emerging technology enabled threats.

Recommendation 21 (Paragraph 94): The UK should seek to play a leading and proactive role in shaping the Global response to TNR as part of the US chaired Working Group on Transnational Repression. The Government should also raise the issue at the next Commonwealth Heads of Government Meeting, scheduled to take place in 2026 in Antigua and Barbuda.

Response:

1. The UK Government is committed to working with likeminded international partners, through bilateral and multilateral channels, to raise awareness of TNR and strengthen collaboration and resilience to TNR, encompassing the areas laid out in the report recommendations. For example, in October 2024, the UK Home Office co-chaired a multilateral meeting with the US Department of Justice at the US Embassy in London, focused on addressing state- sponsored high-harm physical threats and other forms of TNR.

2. At the June 2025 G7 leaders' summit, the Prime Minister supported the first G7 statement on TNR. This statement underlined the UK's commitment to strengthen our work with G7 partners to build our collective resilience to TNR in order to keep our communities safe, to defend human rights, and to safeguard our sovereignty.
3. The UK Government is committed to delivering the initiatives outlined in this June G7 statement, working closely with Canada and other G7+ partners. This includes enhancing information sharing through a TNR Resilience and Response Framework in the G7 Rapid Response Mechanism (RRM). Information sharing through this forum and others, is key to building our collective resilience to TNR.
4. We are committed to working with international partners to support those targeted by TNR, including in the online domain. As outlined in the June 2025 G7 statement on TNR, the UK, alongside Canada, have established the Common Good Cyber Fund to support victims of TNR. We have also been supporting the development of the G7 Digital TNR Academy which will support with strengthening the UK's and G7 partners technical skills and tools for identifying and responding to the latest technology-enabled threats.
5. We have shown leadership, with international partners, through issuing joint statements in response to TNR activity. For example, in July 2025 the UK and 13 likeminded partners issued a statement underlining our opposition to the attempts of the Iranian intelligence services to kill, kidnap, and harass people in Europe and North America. Additionally, in August 2025, the UK supported a joint statement, alongside G7 RRM partners, condemning the latest round of arrest warrants issued by the Hong Kong Police Authorities as TNR, and underlined our commitment to support those targeted. Statements such as these, help to increase awareness of TNR activity and raise the barriers and costs for perpetrator states carrying out this activity.
6. The UK Government has also been working with likeminded partners to raise awareness and strengthen collaboration through the UN to build collective resilience to TNR. We regularly engage with UN organisations on TNR and supported a joint statement on TNR alongside likeminded countries at the UN Human Rights Council in July 2024, the first multilateral statement focused specifically on TNR at the UN. The UK Government has also supported efforts at the UN to call out preparators of TNR activity. For example, at UNHRC59 the UK supported a resolution on the Eritrean human rights situation, which included expressing concern over TNR activity.
7. The UK will continue to utilise bilateral and multilateral opportunities to raise awareness and strengthen collaboration to build collective resilience to TNR.

Recommendation 22 (Paragraph 97): We recommend this new unit has a central role in coordinating the UK's response to TNR, ensuring that intelligence, law enforcement, and policy functions are aligned and responsive to emerging threats. We recommend the appointment of a dedicated lead for transnational repression within the unit, responsible for driving cross-government coordination.

Response:

1. We agree with the Committee's findings that structured and consistent coordination across government is key to countering TNR, and it has been a priority to ensure our approach is joined up across departments, with formalised mechanisms for collaboration. The UK's strategic approach to TNR has been shaped by the comprehensive review undertaken by the Defending Democracy Taskforce. The Defending Democracy Taskforce coordinates and drives forward a whole-of-government response to the full range of threats to our democracy. It comprises Ministers and senior officials from multiple government departments, alongside representatives from law enforcement, the Parliamentary authorities, and the UK Intelligence Community.
2. Collaboration across Government, law enforcement and agencies is essential in countering TNR. The TNR Review - in bringing together a wide range of government departments and agencies to ensure full coherence in our response - is a good example of the depth of this collaboration. This review brought together officials from lead government departments, law enforcement, the intelligence and security services, and civil society partners to build a shared understanding of the threat and evaluate the UK's existing response.
3. As announced in the Security Minister's Written Ministerial Statement on 14 May, a dedicated team has now been established within the Home Office to act as the central point of coordination for TNR across government. This team will oversee the UK's overarching strategy on TNR, working with departments, operational partners, and civil society to ensure that our response remains proportionate, protective and evidence led.
4. The Home Office TNR team will work closely with the newly established State Threats Joint Unit, which has been created to deliver on the Government's manifesto commitment to better counter hostile activity by state actors. That unit will play three key roles: first, it will drive delivery across government to counter state threats, building on the successful model of the counter- terrorism system to deliver strategic outcomes. Second, it will embed a 'whole of society' approach, enabling Government to have more effective public conversations about state threats, forging partnerships with industry, academia and like-minded states. Third, it will establish

a UK Centre of Excellence on state and hybrid threats, bringing together expertise within government and collaborating with external experts to set the research and policy agenda.

5. We recognise the importance of the specific roles and responsibilities of each department in responding to TNR. As the department primarily responsible for maintaining law and order, protecting national security, overseeing immigration policy and ensuring the safety of communities in the UK, the Home Office owns the UK's response to TNR. While the Home Office leads on domestic security and related levers, the FCDO plays a critical role in diplomatic engagement (including through work in multilateral fora such as the G7 RRM) and promoting human rights, and the policing and intelligence services contribute vital operational and investigative capabilities. These functions are coordinated through both formal and informal governance mechanisms, which enable a coherent and agile response to emerging threats.