

# PARLIAMENTARY DEBATES

HOUSE OF COMMONS  
OFFICIAL REPORT  
GENERAL COMMITTEES

## Public Bill Committee

### NATIONAL SECURITY BILL

*Seventh Sitting*

*Tuesday 19 July 2022*

*(Morning)*

---

#### CONTENTS

CLAUSES 27 to 32 agreed to.  
SCHEDULE 4 agreed to.  
CLAUSES 33 and 34 agreed to.  
Adjourned till this day at Two o'clock.

---

No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor’s Room, House of Commons,

**not later than**

**Saturday 23 July 2022**

© Parliamentary Copyright House of Commons 2022

*This publication may be reproduced under the terms of the Open Parliament licence, which is published at [www.parliament.uk/site-information/copyright/](http://www.parliament.uk/site-information/copyright/).*

**The Committee consisted of the following Members:**

*Chairs:* RUSHANARA ALI, † JAMES GRAY

- |  |  |
|--|--|
| † Bell, Aaron ( <i>Newcastle-under-Lyme</i> ) (Con)    | † McDonald, Stuart C. ( <i>Cumbernauld, Kilsyth and Kirkintilloch East</i> ) (SNP) |
| Eagle, Maria ( <i>Garston and Halewood</i> ) (Lab)     | † Mann, Scott ( <i>North Cornwall</i> ) (Con)                                      |
| † Elmore, Chris ( <i>Ogmore</i> ) (Lab)                | Mohindra, Mr Gagan ( <i>South West Hertfordshire</i> ) (Con)                       |
| † Everitt, Ben ( <i>Milton Keynes North</i> ) (Con)    | † Mumby-Croft, Holly ( <i>Scunthorpe</i> ) (Con)                                   |
| † Hart, Sally-Ann ( <i>Hastings and Rye</i> ) (Con)    | † Phillips, Jess ( <i>Birmingham, Yardley</i> ) (Lab)                              |
| Higginbotham, Antony ( <i>Burnley</i> ) (Con)          | Sambrook, Gary ( <i>Birmingham, Northfield</i> ) (Con)                             |
| † Hosie, Stewart ( <i>Dundee East</i> ) (SNP)          | Huw Yardley, Bradley Albrow, Simon Armitage,<br><i>Committee Clerks</i>            |
| † Jones, Mr Kevan ( <i>North Durham</i> ) (Lab)        | † <b>attended the Committee</b>  |
| † Jupp, Simon ( <i>East Devon</i> ) (Con)              |  |
| † Lynch, Holly ( <i>Halifax</i> ) (Lab)                |  |
| † McPartland, Stephen ( <i>Minister for Security</i> ) |  |

## Public Bill Committee

Tuesday 19 July 2022

(Morning)

[JAMES GRAY *in the Chair*]

### National Security Bill

9.25 am

**Mr Kevan Jones** (North Durham) (Lab): On a point of order, Mr Gray. I wrote to Mr Speaker about new clause 6, which was tabled in my name, to ask whether it was in order. I understand that that the decision was then passed to you and Ms Ali, the Chairs of the Committee. Have you have contemplated the new clause, is it in order, and will it be discussed later?

**The Chair:** I am most grateful to the right hon. Gentleman for his point of order. He is right: his new clause has been received and we have been contemplating the matter for some time. The question is whether the subject of new clause 6 is in scope, and learned authorities have different views on that. Some, including the previous Lord Chancellor, believe that it is in scope, while others believe that it is not.

Mr Speaker ruled that it is for my co-Chair—the hon. Member for Bethnal Green and Bow—and I to decide. We have taken the view that we are not legal experts and are therefore unable to judge correctly whether the new clause is in scope, but that the business of this place is to debate things rather than to stifle debate, so without commenting on whether the matter is in scope, we believe that it should be debated. If the Government do not like it, they can vote it down in Committee or at a later stage, but deciding that the clause is out of scope would be beyond our pay grade. We have taken the view that the new clause will indeed be in scope and that we can debate the public interest defence.

**Mr Jones:** Further to that point of order, Mr Gray. I thank you and Ms Ali for your consideration of the new clause.

#### Clause 27

##### INTERPRETATION

*Question proposed,* That the clause stand part of the Bill.

**The Chair:** Amendment 48 to clause 27 was debated earlier on, but I understand that its proposer does not wish to press the amendment to a vote. Is that right?

**Stuart C. McDonald** (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP) *indicated assent*.

**The Chair:** If people wish to debate the clause, we can do so now.

**Stuart C. McDonald:** I do not intend to detain the Committee long on this interpretation clause, but I think it might contain a typo, because it states:

“‘foreign power threat activity’ and ‘involvement’, in relation to such activity, have the meaning given by section 27”.

This will be section 27, so that is rather circular. I think it should read “the meaning given by section 26”, because clause 26 defines “foreign power threat activity” and “involvement”. I just wanted to point out that possible typo, which the Minister may want to consider.

**The Chair:** I am sure that the Minister, the Clerks and I are most grateful for that point. I certainly cannot answer it immediately, and the Minister does not look as if he is going to—

**The Minister for Security (Stephen McPartland):** I am grateful to the hon. Gentleman for pointing out that typo. That is very important to us all, and I will carry on talking while I wait for some information. I think that is an important point. As we know, the Bill is evolving and will continue to evolve. We will ensure that any potential errors are corrected throughout its passage. It does look as though it should say “section 26”, so we will definitely fix that.

**Jess Phillips** (Birmingham, Yardley) (Lab): We had all noticed.

**Stephen McPartland:** I am grateful to the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East for his eagle eyes.

**The Chair:** The learned Clerk also agrees that it should read “section 26”. We are most grateful to the hon. Gentleman for pointing that out.

*Question put and agreed to.*

*Clause 27 accordingly ordered to stand part of the Bill.*

#### Clause 28

##### OFFENCES BY BODIES CORPORATE ETC

*Question proposed,* That the clause stand part of the Bill.

**Holly Lynch** (Halifax) (Lab): Clause 28 deals with offences committed by bodies corporate. It is a significant clause. I imagine that this legislative area will continue to need to evolve as threats continue to emerge. The clause asserts that where a corporate body commits an offence under part 1 of the Bill

“the officer, as well as the body, is guilty of the offence”.

Finding the right balance here will not be straightforward, but this will become a key battleground, as the Government acknowledged with the National Security and Investment Act 2021.

In its report, the Law Commission outlined that classified evidence, which it was considering, could be explained using the following hypothetical example. P, an IT services company headquartered in a foreign state, has a managed services contract for a large Department. As part of that contract, P creates back-ups in the UK of the Department’s corporate email and file

storage system. P is compelled under the foreign state's national security legislation to share that information with the foreign state's intelligence services, which use it to target UK interests. Worryingly, that will not be an uncommon scenario; we see such examples regularly in the UK press, and a range of stakeholders need to be alive to the risks. I am afraid to say that the Government have been too slow to respond.

In December 2020, the US Department of Homeland Security issued a data security business advisory, which “describes the data-related risks American businesses face as a result of the actions of the People's Republic of China (PRC) and outlines steps that businesses can take to mitigate these risks. Businesses expose themselves and their customers to heightened risk when they share sensitive data with firms located in the PRC, or use equipment and software developed by firms with an ownership nexus in the PRC, as well as with firms that have PRC citizens in key leadership and security-focused roles...Due to PRC legal regimes and known PRC data collection practices, this is particularly true for data service providers and data infrastructure.” The advisory was issued as a result of several new laws passed in China in recent years—not least the national intelligence law of 2017, which compels all PRC firms and entities to support, assist and co-operate with PRC intelligence services, creating a legal obligation for those entities to turn over data collected abroad and domestically to the PRC.

A UK employee working for a Chinese company will need really robust legislative support in pushing back against the obligations placed upon Chinese businesses by those new laws under the Chinese Communist party. For that reason, we welcome clause 28, and believe that the provisions are sufficiently broad to include anyone in a company who may commit an offence under part 1 of the Bill, and to provide clarity in this space, with a need to consider employees who stand to find themselves in a difficult position due to the Chinese legislative framework.

Subsection (5) will allow the Secretary of State to make regulations to improve the clause through secondary legislation. I have said that I recognise that legislation will need to be dynamic if it is to be effective, but any such regulations should be laid under the affirmative procedure, and must be debated and actively approved by both Houses of Parliament. I hope the Minister will confirm that that will be the case.

**Stephen McPartland:** The clause provides that where a body commits an offence under part 1 of the Bill “the officer, as well as the body, is guilty of the offence”

if it is attributable to the officer's consent, connivance or neglect. The provision is based on a similar one in the Official Secrets Act 1911. For example, where a body commits an espionage offence of obtaining protected information under the direct guidance of the head of the body, both the body and its head would be guilty of the offence. Clause 28 mirrors the provisions found in section 36 in part 3 of the National Security and Investment Act 2021, which makes suitable provision for when an offence under that part is committed by a body corporate.

It is worth noting that in a similar provision in the 1911 Act, a director would automatically be held liable unless they could prove that they did not consent or were unaware. Rightly, the provisions move beyond that burden of proof: the prosecution must now demonstrate beyond reasonable doubt that an officer was culpable in

such a case, which provides more safeguards. This is therefore an important provision to ensure that both companies and relevant officers can be held liable for their involvement in state threat activity, and that where there is wrongdoing on the part of an officer of the company that officer can be appropriately prosecuted for the offences.

For an officer to be held liable, they must consent or connive to the act or be negligent in relation to it, which is a higher bar than simply being unaware of the act, as the prosecution would need to demonstrate not just a lack of awareness but that, in being unaware, the person was failing to properly discharge their duties. The clause goes on to define a number of terms, such as a “body” and an “officer of a body”, and it provides that the Secretary of State may make regulations to modify the section in relation to

“its application to a body corporate or unincorporated association formed or recognised under the law of a country or territory outside the United Kingdom.”

That may be required as a result of differences in the nature of bodies corporate, their structures or their terminology under the laws of foreign jurisdictions. This ensures that bodies corporate outside the UK that commit offences under part 1 of the Bill can still be caught under these offences.

I will refer to the example given by the hon. Member for Halifax. We have tried throughout the Bill to demonstrate that the offence will be based on an individual acting directly or indirectly on behalf of a foreign power, and on whether they should reasonably know that that behaviour is on behalf of a foreign power. I understand her point about foreign-owned companies, but the Bill does not say that whole companies are acting on behalf of a foreign power. As she rightly says, there will be a whole range of UK individuals engaged in completely legitimate activity within the UK, and we do not want to give employees of those companies any problems.

The regulations will involve technical, rather than substantial, changes, so they will not widen the scope whatsoever. That is why they will be made under the negative procedure.

*Question put and agreed to.*

*Clause 28 accordingly ordered to stand part of the Bill.*

*Clause 29 ordered to stand part of the Bill.*

### Clause 30

#### CONSENTS TO PROSECUTIONS

**Stuart C. McDonald:** I beg to move amendment 63, in clause 30, page 23, line 16, at end insert—

“(c) in Scotland, only with the consent of the Lord Advocate.”

*This amendment would require the consent of the Lord Advocate to prosecute certain offences.*

**The Chair:** With this it will be convenient to discuss clause 30 stand part.

**Stuart C. McDonald:** Clause 30 puts in place one of the protections that the Minister has referred to a few times, including when we were debating the offences of

[*Stuart C. McDonald*]

disclosure and the breadth of the foreign power condition. The protection in question is the requirement of consent to certain prosecutions, with that consent coming from the Attorney General in England and Wales, and from the Advocate General in Northern Ireland.

Our amendment 63 simply asks why there is no equivalent requirement of consent from the Lord Advocate for prosecutions in Scotland. It might be a conscious choice—if so, it would be useful to hear what the thinking is behind that. It could also be another mistake, because I notice that section 8 of the 1911 Act requires consent to prosecution, but only the Attorney General is mentioned. Section 12, which provides an interpretation, states that the expression “Attorney General” is taken “as respects Scotland” to mean the Lord Advocate, and “as respects Ireland” to mean the Advocate General for Northern Ireland. That is a slightly dated way of doing things, because if we mean the Lord Advocate, we should say that.

On the clause itself, I have absolutely no objection to the idea that consent for prosecution is an appropriate step. As I say, our amendment simply asks what the provision is in relation to Scotland.

**Stephen McPartland:** Let me quickly answer those points. Clause 30 provides that the consent of the Attorney General is required in England and Wales, and that the consent of the Advocate General is required in Northern Ireland. I understand that the Lord Advocate is not included because the Lord Advocate has a constitutional role as the head of the criminal prosecution system under the Criminal Procedures (Scotland) Act 1995, and all prosecutions on indictment are taken by, or on behalf of, the Lord Advocate. It is technically not necessary to include the Lord Advocate, because all offences in relation to Scotland are prosecuted by the Lord Advocate under Scots law, so I ask the hon. Gentleman to withdraw the amendment.

**Stuart C. McDonald:** Very educational; I have learned something new. I am grateful to the Minister for his explanation, and I beg to ask leave to withdraw the amendment.

*Amendment, by leave, withdrawn.*

*Clause 30 ordered to stand part of the Bill.*

### Clause 31

POWER TO EXCLUDE THE PUBLIC FROM PROCEEDINGS

*Question proposed,* That the clause stand part of the Bill.

**Holly Lynch:** I wish only to add that I imagine we would all agree that transparency in this legislative area should be the default, especially given the need to raise awareness of the challenges we face as a country and the individual responsibilities that we all share in combating those challenges with the arrival of these new offences. That said, it is of course right that clause 31 provides power to the court to exclude the public from any part of proceedings or offences under part 1, or for proceedings

relating to the aggravation of sentencing, or other offences where the foreign power condition applies, should the evidence being considered deem it to be in the interests of national security to do so.

**Stephen McPartland:** As the hon. Member said, clause 31 provides those protections. It builds on the Official Secrets Act 1920, which gives the court the power to exclude the public from any proceedings if the publication of any evidence to be given would be prejudicial to national security. However, the passing of the sentence must still take place in public.

One important point is that the decision to exclude the public will be made by the court, not the prosecution. It is also important to reiterate that the power does not grant the use of closed-material proceedings. Therefore, as is the precedent in our criminal justice system, the defendant and their legal team will have access to all the evidence, as they would in other criminal proceedings.

I will end by reassuring the Committee that the clause is not meant to limit the transparency of our justice system or the independence of the judiciary, but to ensure that—only where necessary—the courts themselves have the power to protect the United Kingdom’s national security.

*Question put and agreed to.*

*Clause 31 accordingly ordered to stand part of the Bill.*

### Clause 32

POWER TO IMPOSE PREVENTION AND INVESTIGATION MEASURES

*Question proposed,* That the clause stand part of the Bill.

**The Chair:** With this it will be convenient to discuss the following:

Amendment 57, in schedule 4, page 111, line 1, leave out paragraph 12.

*This amendment would remove the power to require participation in polygraph sessions.*

That schedule 4 be the Fourth schedule to the Bill.

**Holly Lynch:** Clause 32 is the first clause of part 2, and introduces the state threat prevention and investigation measures, or STPIMs, replicating the terrorism prevention and investigation measures, or TPIMs, framework, which is already in existence. Like TPIMs, STPIMs impose significant restrictions on a person’s freedoms without that being the consequence of a crime having been committed and tried before the courts.

Schedule 4 sets out a list of the types of measures that may be imposed on an individual under this part. The Secretary of State may impose any or all the measures that he or she reasonably considers necessary, for purposes connected with preventing or restricting the individual’s involvement in foreign power threat activity.

Taken cumulatively, the measures will restrict the freedoms of the STPIM subject in a way that is normally possible only during criminal or immigration proceedings, or restrictions under the Mental Health Act 1983. Inevitably, we are looking for assurances that measures of this kind

are necessary and effective, especially as the threshold for applying an STPIM is naturally lower than the threshold for a criminal conviction.

In considering the balance, we have looked to the efficacy of TPIMs as a starting point, and at the invaluable work of the independent reviewer of terrorism legislation, Jonathan Hall QC, who provides an ongoing assessment in his annual review. According to the latest independent annual review of terrorism legislation, between the Terrorism Prevention and Investigation Measures Act 2011 receiving Royal Assent and 31 December 2020, only 24 individuals were served with a TPIM notice. That would suggest that they are not used often.

In 2020, all but one of the TPIMs in force were against members of the proscribed terrorist network ALM—al-Muhajiroun. The report makes clear that ALM's direct or indirect impact on UK terrorism includes the 2013 murder of Fusilier Lee Rigby, the 2017 London Bridge Attack and the 2019 Fishmongers' Hall attack. That underlines the severity and level of risk that those measures are seeking to manage and suppress, when considering the terrorism equivalent.

Jonathan Hall was asked whether he thought the STPIMs might be used more readily than TPIMs when he gave evidence in the Committee's first session. He said,

"if the regime operates as it is intended to, because the Bill replicates the obligation for the Secretary of State to consider whether it is possible to prosecute in the first place. I do not think in practice that they will become a measure of first resort, just because they are so resource-intensive and complicated."—[*Official Report, National Security Public Bill Committee, 7 July 2022; c. 10, Q16.*]

When asked about the efficacy of STPIMs, he said,

"I expect that they will be effective because the agencies and the Home Secretary will only think about imposing one when they think it is going to work."—[*Official Report, National Security Public Bill Committee, 7 July 2022; c. 6, Q6.*]

We are reassured by Jonathan Hall's contributions in that first session of the Committee. We will revisit some of his other comments in debates on other clauses, particularly around oversight in clause 49 and the ongoing review process under clause 40.

9.45 am

On schedule 4, there is uncertainty about who might be issued with a part 2 notice, so I am speculating, but given that all TPIMs subjects in 2020 were British nationals, does the Minister envisage that there will be more foreign nationals among those subject to STPIMs? How will the provisions in part 2 interact with the Government's immigration controls?

Jonathan Hall said in evidence that STPIMs were unlikely to ever become a tool of first resort,

"just because they are so resource-intensive and complicated."—[*Official Report, National Security Public Bill Committee, 7 July 2022; c. 10, Q16.*]

Although I understand that counter-terrorism police lead on the enforcement of TPIMs, for obvious reasons, with a regional CT hub and support from the regional police force, who will lead on the enforcement of STPIMs? Will it be the intelligence community, counter-terrorism policing or regional police forces?

When speaking to the differences between terrorist and state threats, Jonathan Hall said that

"unlike some of the terrorist TPIM subjects who are individuals without a huge amount of access to resources, some of the individuals who may be under an STPIM could be backed by a huge amount of resources".—[*Official Report, National Security Public Bill Committee, 7 July 2022; c. 10, Q16.*]

I hope the Minister can assure us that the right agencies, with an understanding of those resources, will be dedicated to monitoring and enforcing compliance with a STPIM, in order for it to be effective.

Paragraph 5 of schedule 4, which covers restricting access to cash and financial services, makes no mention of cryptocurrency. Microsoft's "Digital Defense Report" notes that nation state actors from North Korea added monetary gain to their motives for cyber-attacks. It says:

"North Korea targets companies in cryptocurrency trade or related research, likely seeking either to steal cryptocurrency or intellectual property. North Korea's economy is never strong, but the COVID-19 pandemic coming after years of UN sanctions has pushed it to its worst state in a generation, forcing North Korea to seek to find money by any means necessary."

The BBC reported in January this year claims that North Korean hackers stole almost \$400 million, or £291 million, of digital assets in at least seven attacks on cryptocurrency platforms in the previous year. We know cryptocurrency is a particular focus for some hostile states, so why are we not adding cryptocurrency to the list in paragraph 5(6)?

SNP amendment 57 would remove the power to require participation in polygraph sessions. I asked Jonathan Hall about that issue, having read his assessment of polygraphs in his annual review, where he said that

"a power to add a polygraph measure was added. No regulations have yet been made for the conduct of TPIM polygraph sessions. Evidence from TPIM polygraph sessions is expressly excluded from criminal proceedings, but, although the government stated that the provision 'is not designed to allow for information derived from a polygraph examination to be used as evidence in proceedings for breaching a TPIM (which is a criminal offence), to extend the duration of a TPIM notice, or to impose a new TPIM', and indeed that 'any attempt to use information derived from a polygraph examination to extend the duration of a TPIM notice would be unlawful', there is no statutory bar as such. I expect the Home Office to draw to my attention any case in which polygraph evidence obtained under compulsion is sought to be introduced (in any manner) into TPIM proceedings, so I can consider the position in next year's report."

That all sounds a bit messy, and that is why I was keen to ask about polygraphs during the evidence session. I asked Mr Hall whether he had been able to consider their use in any ongoing cases. He said:

"What I have been told is that polygraphs have not been used for TPIMs, as far as I am aware, but they have been used for released terrorist offenders and some disclosures have been made. Everyone always thought that the real utility of polygraphs and the clear reason for their use is the disclosures that people make when undergoing the process. I gather that some admissions have been made that have been valuable and have led to a recall. I do not have a huge amount of data, but they seem to have had some success in the context of terrorism offences."—[*Official Report, National Security Public Bill Committee, 7 July 2022; c. 7, Q7.*]

For that reason, we will be following their use carefully and will await a proper assessment of the use of polygraphs in the next annual review; I hope the Minister can be clear about how he envisages them working.

**Sally-Ann Hart** (Hastings and Rye) (Con): There have been several reviews of polygraph accuracy, and they are accurate about 80% to 90% of the time. Although

[Sally-Ann Hart]

they are far from foolproof, they can detect lies, thoughts and intentions to deceive. They are already used in the UK for probation purposes, and their use can encourage people to tell the truth. Along with the other measures in the Bill, they will have their use.

**Stuart C. McDonald:** As the shadow Minister, the hon. Member for Halifax, set out, clause 32 introduces the power to impose STPIMs on an individual via a part 2 notice, and schedule 4 sets out the types of measure that can be imposed.

As I argued on Second Reading, none of us should ever feel comfortable about curtailing people's liberties via administrative civil orders rather than as punishment for crimes that have been proven through trials. None the less, we acknowledge that such prevention and investigation measures are a necessary and useful part of combating terrorism, and our position on TPIMs has been to focus on trying to clip their wings, improve oversight and limit their invasiveness, rather than to oppose their use altogether.

We think that the balance of evidence shows a similar case for STPIMs. However, we should again be careful in our scrutiny of them, and not permit interference in people's liberties without proper justification and appropriate limits and oversight. We welcome, for example, that the residence measures in paragraph 1 to schedule 4, which are among the most restrictive measures set out in that schedule, apply only to individuals who are thought to be involved in the most immediately serious activity. Some of the measures are broad, but they seem to be curtailed and properly restricted by the provisions in clause 33—which we will discuss shortly—ensuring that they cannot go beyond what is necessary, although we have some concerns about the various tests that the Secretary of State has to require before applying the measures.

As the Committee has heard, amendment 57 would take out paragraph 12 of schedule 4, on the use of polygraph tests as a means of assessing compliance. Our view is that as polygraph tests remain too unreliable and lack an evidence base, they are inappropriate tools for measuring compliance with STPIMs, especially in the light of all the other means at the Secretary of State's disposal, including the monitoring measures in paragraph 15 of schedule 4, as well as the full range of investigatory powers that the services have at their disposal. It is hard to see what paragraph 12 will add. As the shadow Minister said, polygraph tests are not currently used at all.

If there is a case for the use of polygraph tests and the Minister is keen to retain the power to impose such a condition, I ask him to consider removing their applicability in Scotland. There is a precedent for that: polygraphs were introduced for TPIMS in the Counter-Terrorism and Sentencing Act 2021, but during the Act's passage, the Scottish Government indicated that they would not promote a legislative consent motion for polygraphs on the basis that, because polygraph testing is not currently used at all in the criminal justice system in Scotland, the fundamental change of introducing them should be a matter of principle to be determined by the Scottish Parliament.

The SNP welcomed the decision by the then Justice Secretary, the right hon. and learned Member for South Swindon (Sir Robert Buckland), who is now the Secretary of State for Wales, to remove the provisions on polygraphs that applied to Scotland. Following that concession, a legislative consent motion was eventually approved at Holyrood. If I recall correctly, the Northern Ireland Executive expressed similar concerns. We see no case for polygraphs, but we assume that the Minister does, and if he wishes to retain their inclusion in the Bill, we respectfully ask that he take the same approach as his right hon. and learned Friend by not applying the provisions to Scotland.

**Mr Jones:** I support the measures because they are an extra weapon in the armoury to fight against hostile state intervention in this country. Clearly, the arguments about the level to which the restrictions will be imposed are very complex. There will be cases in which the prosecution test will not be met but we still have evidence about individuals.

My only problem with the measures is in relation to how they will be used practically. As we all know, TPIMs have not exactly been uncontroversial in their prosecution. Will the Minister give us an understanding of how they will be used and in what circumstances? If the evidence is there—and I accept that sometimes that will be difficult, in the sense that a lot of evidence against individuals will be unable to be put in the public domain—when will the measures be used, and for what duration? That would give people some assurance that they will not be used for lengthy periods against individuals. I accept that in a number of cases the evidential test for prosecution will not be met, and therefore the measures may well be a useful tool in the armoury, but we need some oversight of how they will be used and their effectiveness.

On polygraphs, I have some sympathy with the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East. Interestingly, the hon. Member for Hastings and Rye seems to be answering for the Minister; I do not know whether she is auditioning for the job, but I thought it was the Minister who replied to such things.

I think the jury is out, not just in this country but internationally, on the effectiveness of polygraphs. If we are to ensure that they will not be challenged legally, we could put something in the Bill. I am not suggesting for one minute that polygraphs be used on every occasion, but if one is used in a case that is then thrown out because of the unsafeness of the test, that would unfortunately weaken the tool. The Minister has to justify it. As I say, I would be interested to know about the oversight, and how long he envisages their being used.

**Stewart Hosie (Dundee East) (SNP):** It is a pleasure to serve under your chairmanship, Mr Gray. I have a question on paragraph 8 to schedule 4, entitled "Electronic communication device measure". It is eminently sensible, when one is considering how an STPIM might be constructed, that one looks at all the restrictions that that may involve. However, when we get to sub-paragraph (6)(c), which refers not to computers or telephones but to other equipment "designed or adapted, or capable of being adapted, for the purpose of connecting to the internet," I want to ensure that there is clarity, and that the provision will be defined in a cogent way.

As we move further into the internet of things, one's fridge or toaster will be designed for the purpose of connecting to the internet. That might sound glib or flippant, but we may get to the point when half the white goods in any individual's home are internet enabled. Given that there could be huge sensitivities in the deployment of STPIMs, the last thing that we want to see is a police constable or bailiff removing half the items from someone's house, when that clearly is not the intention but those items nevertheless fit the category in paragraph 8(6)(c).

**Stephen McPartland:** I am grateful for Members' contributions and look forward to trying to answer as many of the questions as I can. I will start with the clause and then come to the amendment and some of the questions.

Part 2 and clause 32 mirror the Terrorism Prevention and Investigation Measures Act 2011—TPIM—and allow the Secretary of State to impose by notice

“specified prevention and investigation measures on an individual” if specific conditions are met; I will refer to them as STPIMs going forward. The STPIMs mirror the equivalent counter-terrorism measures: well-established tools that have been in use for over 10 years and have been subject to vigorous examination by the courts, including with regard to European convention on human rights compliance. The courts have never found that a TPIM in its entirety should not have been imposed, or that any of the provisions of the TPIM legislative framework are not ECHR compliant. That should give us all reassurance, and give Parliament confidence that the measures will be applied sparingly and only where necessary and proportionate.

I will not go through the exhaustive list, but the Government have publicly committed to provide operational partners with the tools that they need to combat state threats. To be very clear, STPIMs are a tool of last resort; the Government's preference is to prosecute under any means possible first and foremost, and STPIMs are to be used only when all else has failed and no other options are available to us. I hope that that provides some reassurance as well.

10 am

**Holly Lynch:** I was reassured by some of the detail in these clauses about that point, but the impact assessment from the Home Office says:

“It is assumed that the prosecution rate of state threats investigations is 33 per cent. This is an internal estimate from CPS, based on prosecution of previous OSA 1911-1939 cases.”

Based on where we envisage we might have challenges in securing prosecutions, I wonder whether STPIMs are also for the other side of a prosecution, as well as for when we cannot secure prosecution and get there in the first place.

**Stephen McPartland:** I am grateful to the hon. Lady for that point. I understand that our responsibility is to scrutinise the legislation to make sure that, as the hon. Member for Dundee East made clear, we do not open up a can of worms that can lead to greater and greater unintended consequences, but the reality is that the provision is to be a last resort.

If we are talking practically, counter-terrorism police are responsible for enforcing STPIMs. The amount of resources required to enforce and monitor a TPIM or STPIM is so great and so large that, as Members can imagine, it is not something that any of the agencies or anybody in Government wants to do, so it is not something that we will look to push. First and foremost, this is about prosecution by any means possible.

To give some kind of hope and clarity, I would like to make the point that the number of TPIMs currently in use is less than four. The number of TPIMs that have been used throughout the 10 years of their existence is less than the clause number that we started on today. I hope that gives some reassurance on how limited the measures will be, and on how few occasions they will be used.

We have been looking at the specific time limit, and we are including a specific condition to have a maximum of five years for the duration of an STPIM. Again, that is to mirror what is in the TPIM legislation. Additionally, subsection (4) requires the Secretary of State to publish factors that she considers are appropriate to take into account when deciding whether to restrict a person's movement in the UK—for example, ensuring that they have access to appropriate medical facilities.

Part 1 to schedule 4 sets out 16 measures. Right hon. and hon. Members will know there are 17 measures in TPIM legislation for differences around drug testing, but we do not believe that is applicable in this case. The measures have to be tailored to the specific threat that an individual poses.

I want to touch on the polygraph measure, as it has been raised by a number of colleagues. It is designed to allow the Secretary of State to require an individual to take a polygraph test at a specific date, time and location. The purpose of the measure is to assist operational partners to assess whether an individual is complying with the other measures under their STPIM. The outcome of the session may be used to make changes to the individual's suite of measures—for example, removing or adding specific measures to prevent or restrict their involvement in state threat activity. Again, this measure is expected to be used exceedingly rarely.

Let me reassure the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East that the polygraph session cannot under any circumstances be used to gather evidence for a future prosecution. I am stating on the record that polygraph measures cannot be used to gather evidence for a future prosecution, and I hope that that provides reassurance.

**Mr Jones:** I am grateful for that clarification, but what happens if someone gets a negative polygraph test and has actually broken their STPIM? Surely it will be used as an evidential test, because they have not complied with their conditions.

**Stephen McPartland:** Under the way the law system works, that might provide some kind of information, but it will not be used as evidence. The operational partners would then have to go off and identify the evidence in order to find out how they could do that, because breaching a notice is a criminal offence, so they would need the evidence in order to then go to court to demonstrate that.

**Mr Jones:** I understand what the Minister is saying, but I have a real problem with this; I think the Government are opening up an argument for lawyers who want to defend people. Obviously, if somebody is prosecuted for breaking an STPIM, then in discovery, the lawyer is going to ask, “Was a polygraph test done? Does the individual know they have done it?” I am worried about putting this in, because there is a controversy about polygraphs allowing the defence an opportunity to undermine the process. I understand why the Bill is belt and braces, but I am not sure that this part of it is going to be helpful.

**Stephen McPartland:** I am grateful to the right hon. Member for his point, and I understand it, but polygraph measures are currently used in the management of sex offenders in this country, and the Bill will operate very much on the same principles. He should remember that in this legislation we are not trying to create new bits and pieces for controlling an individual; operational partners have found these tools effective over the past 10 years, so we are trying to mirror what is already out there. That is the purpose of the legislation.

The hon. Member for Halifax asked about foreign nationals. Our ambition is to prosecute using any means possible, including deportation, so if that is not available, we would look to use one of the measures in the Bill. Because we would look at deportation and everything else as an option, we would expect the measures in the Bill to apply more to British citizens than they would to foreign nationals. As I have stated, counter-terrorism police are responsible for looking after and enforcing the measures. We talked about the number of TPIMs; I am not allowed to give the exact figure, but I have given an indication of how rarely they are used. We imagine that STPIMs will also be used very rarely.

On the right hon. Member for Dundee East’s point about the internet of things and trying to future-proof the legislation, under paragraph 8 of schedule 4 we can restrict access to electronic devices, and as such restrict access to electronic currencies. We talk about cryptocurrency, but cryptocurrency is already becoming a bit old-fashioned. Before I took on this role, I launched an all-party parliamentary group on digital currency and potential bearer currencies run by central banks; cryptocurrency is already becoming something of the past and we are now moving on to bearer currencies managed by digital banks. It is about safeguarding and future-proofing, and under paragraph 6 we can restrict the transfer of property, so we could restrict a transfer of funds in that way.

**Stewart Hosie:** Before the Minister moves on, can I add to the point that the right hon. Member for North Durham made about polygraph tests? The Minister said that polygraph tests will not be used to secure a criminal conviction; that is true but, as he said, the STPIMs are measures of last resort in lieu of a conviction if it is not possible to secure one. The polygraph measures in paragraph 12(1)(a)(ii) of schedule 4 refer to

“assessing whether any variation of the specified measures is necessary for purposes connected with preventing or restricting the individual’s involvement in foreign power threat activity”.

A STPIM is not a criminal conviction, then, but it is in lieu of a criminal conviction; therefore, the Minister cannot be right when he says the polygraph test would

not be used to do something, because it could well be used to vary the conditions and possibly to toughen the STPIM—

**The Chair:** Order. Interventions should be brief.

**Stewart Hosie:** I just wonder if the Minister could go a bit further on that point.

**Stephen McPartland:** I am grateful to the right hon. Member for highlighting that point; I very much enjoy the suggestions that are made in this Committee. I understand the points he is making, and one of the things I have tried to demonstrate throughout the Bill Committee is my willingness to listen and try to work cross-party to get the legislation through.

**Mr Jones:** I hear what the Minister is saying and I think it is important, but would it be possible for him to write to the Committee when he has given the matter a bit more thought? The point that the right hon. Member for Dundee East has made is pretty important.

**Stephen McPartland:** I am always willing to write to the Committee, as the right hon. Member knows. I am happy to go away, think about this issue and then write to the Committee, so that I can put in writing the safeguard that I do not want a polygraph test to be able to lead to future prosecutions. I think that would work.

**Holly Lynch:** Before the Minister moved to the polygraph point, he was talking about cryptocurrencies and said that they are already quite a dated concept; however, my proposal is that we add cryptocurrencies to the list, in paragraph 5 on financial service measures, that includes postal orders, cheques and bankers’ drafts. With that in mind, it might be worth making an explicit reference in that list to whatever form of digital currency or cryptocurrency, given that we know it is a focus for hostile state activity.

**Stephen McPartland:** The hon. Lady makes a very good point. As she knows, I am always prepared to improve legislation so that we are happy with it on a cross-party basis, it goes through the House and we can support our intelligence communities. I am very happy to look at that issue. I did not even know we could still get postal orders and bankers’ drafts.

Let me give some examples of how STPIMs could be used, specifically for the right hon. Member for North Durham—I know that he would like that. If a British national were recruiting, talent spotting and reporting for a foreign intelligence service, and the evidence to prove the foreign power links was too sensitive to be used in court, meaning that a prosecution was not viable, an STPIM that might prevent harm could include a financial order, to prevent the person from accessing funds from the foreign intelligence service; a restriction on contact or association with individuals, to prevent the person from being debriefed by the foreign intelligence service handler; and electronic communications device measures, to ensure full coverage of devices used by the subject. That is one example of how an STPIM could be used.

Another example relates to a British national working in one of our defence companies, and would prevent sensitive technology transfer. Suppose a disgruntled British national employee of an advanced technology company is seeking to market specialised, valuable and unclassified knowledge to foreign companies. The investigation and disruptive conversation means that the individual is moved to less sensitive work and their company computer access is restricted, but they cannot be dismissed. They remain disgruntled, but prosecution is not viable. In that case, we could disrupt travel to prevent an individual from meeting foreign representatives abroad, so that they could not pass the secrets over to them, and we could restrict contact and association with individuals in the UK for the same purposes.

This example relating to the intimidation of dissidents is particularly important. Suppose a senior member of, for example, a cultural organisation from a foreign Government based in the UK is seeking to exert pressure on dissident diaspora through intimidation, harassment and damaging rumours. The individual cannot be expelled or deported, so victims are afraid to make criminal complaints for fear of recrimination in their home country. The STPIM could be imposed, because prosecution is not viable—the victim will not testify or make a statement. We could put measures in place to prevent an individual from associating with the victim or members of their family. We could prevent serious violence by ordering the subject to relocate to an alternative area in the UK. The STPIM could be justified in closed court proceedings, because it would prevent any identification of the victim. I hope the right hon. Member for North Durham enjoyed those examples.

**Mr Jones:** I did, actually—I am very grateful to the Minister. He has set my mind running in terms of the possible uses of the measures. There is open-source evidence of the intimidation of protesters against the Chinese Government at universities, for example, by Chinese nationals here in the UK. Proving that those individuals were working directly for the Chinese Communist party or a people's front, for example, is difficult. Could the Minister envisage the measures being used to prevent that type of harassment, by individuals who are intimidating or trying to close down legitimate protest against the Chinese Communist party, of legitimate protesters on university campuses?

**Stephen McPartland:** I can genuinely understand and imagine a pathway in which that could be the case. However, as I say, because of the huge amount of resources involved in an STPIM, we will try any other means possible, through normal criminal procedures, to prosecute individuals for harassment under normal criminal law. We will be doing everything we can to not actually use an STPIM. We want to prosecute these people. The Government's first line is prosecution, and the last resort is an STPIM, when there is no other option available to us.

I will also ensure that we add crypto to the list one way or another, but I have to work out how we define it.

*Question put and agreed to.*

*Clause 32 accordingly ordered to stand part of the Bill.*

*Schedule 4 agreed to.*

### Clause 33

#### CONDITIONS A TO E

10.15 am

**Stuart C. McDonald:** I beg to move amendment 55, in clause 33, page 24, line 6, leave out “reasonably believes” and replace with

“believes on the balance of probabilities”.

*This amendment would apply the civil standard of proof in relation to the decision to impose Prevention and Investigation Measures.*

**The Chair:** With this it will be convenient to consider clause stand part.

**Stuart C. McDonald:** Clause 33 sets out the conditions that must be met before a part 2 notice, or an STPIM, can be made. In short, the individual must have been involved in new foreign power threat activity so that the measures imposed by the Secretary of State are necessary, and generally a court then has to give permission.

Amendment 55 revives an earlier argument about the standard of proof that the Secretary of State must apply when assessing whether someone has been involved in activity that requires a prevention and investigation measure. The relevant standard in relation to TPIMs has varied over the years. When TPIMs were first introduced, the requirement was “reasonable grounds for suspecting”, but that was then lifted to “the balance of probabilities”. When the Counter-Terrorism and Sentencing Act 2021 was introduced, the Government sought to take it back down to “reasonable grounds for suspecting”. However, during the passage of that Bill, a compromise was reached in the House of Lords and the test was set at “reasonably believes”. My understanding at the time was that the compromise set a standard not as low as “reasonable suspicion” but not as robust as “the balance of probabilities”, and we took the view that the probabilities test operated perfectly well.

Indeed, Jonathan Hall QC, the Independent Reviewer of Terrorism Legislation, told the Counter-Terrorism and Sentencing Public Bill Committee:

“If it is right that the current standard of proof is usable and fair, and I think it is, in a word, if it ain't broke, why fix it?”  
—[*Official Report, Counter-Terrorism and Sentencing Public Bill Committee*, 25 June 2020; c. 7, Q6.]

At that stage, he was happy with “the balance of probabilities”, and not the Government's original intention to restore the “reasonable suspicion” test. That said, those who accepted that amendment in the House of Lords suggested that the difference between “reasonably believes” and “the balance of probabilities” would be fine, and I acknowledge that far greater legal minds than mine were content with that compromise. Of course, Mr Hall's clear evidence to this Committee was, slightly to my surprise, that to all intents and purposes the balance of probabilities is the same thing as reasonable belief.

Essentially, this comes down to two questions. First, why not just use the tried and tested terminology of “the balance of probabilities” if it is the same thing as reasonable belief? Secondly, does the Minister agree that basically the two tests are the same? I suppose that is the most important question to ask the Minister arising from this amendment.

**Holly Lynch:** I will keep my remarks brief. Conditions A to E, set out in subsections (1) to (5), provide a clear framework that the Secretary of State must work within, with conditions that would then be tested by the court. I listened carefully to my friend the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East. His amendment probes whether clause 33 should apply the civil standards of proof in relation to the decision to impose prevention and investigation measures, by proposing that “reasonably believes” be replaced with “believes on the balance of probabilities”.

In considering that, as the hon. Member said, we look to Jonathan Hall’s evidence in this Committee’s first sitting, and then to the Terrorism Prevention and Investigation Measures Act 2011, and we can see that the wording has pretty much been copied verbatim to this Bill.

With that in mind, and given Mr Hall’s assessment that the measures have not been overused, the lower numbers subject to TPIMs and the reality of just how resource intensive they are, I am satisfied that “reasonably believes” is justifiable, but I look forward to hearing the Minister’s response to the points raised by the SNP spokesperson.

**Stephen McPartland:** Clause 33 mirrors TPIMs, in that it specifies the conditions that must be met in order for the Secretary of State to impose prevention and investigation measures on an individual under an STPIM. Condition A is that the Secretary of State must reasonably believe that the individual is or has been involved in foreign power threat activity. Condition B is that some or all of the foreign power threat activity is new. That ensures that when a notice has expired after the five-year limit provided by clause 34, a further notice may be imposed only where the individual has re-engaged in further foreign powers threat activity since the start of the five-year period.

Conditions C and D outline the two limbs of the necessity test for imposing the measures, so the Secretary of State must reasonably consider, first, that the notice is necessary for protecting the UK from the risk of foreign power threat activity, and secondly, that it is necessary to prevent or restrict the individual’s involvement in foreign power threat activity by imposing the specific measures.

Those two conditions provide an important safeguard that makes it clear not only that must it be necessary in general terms to impose measures on the individual, but that, in addition, each individual measure that is imposed must be necessary in its own right. Condition E requires the Secretary of State to have obtained the court’s permission before imposing measures on an individual. The function and powers of the court on such an application are set out in clause 35.

In urgent cases in which the Secretary of State considers that measures must be imposed immediately, the case must be referred to court for confirmation immediately after measures are imposed. In practice, we expect the emergency power to be used very rarely. The conditions are designed to ensure that STPIMs are used only where they are necessary and proportionate, and they cannot be imposed arbitrarily. There are also several stages at which the courts will be involved in the STPIM process, including granting permission before a notice may be

served or confirming one that has been made in an urgent case. The automatic substantive review of the decision to impose the STPIM and all its obligations and a right of appeal against decisions taken in relation to the STPIM provide checks and balances to the decisions taken by the Secretary of State, so I encourage fellow members of the Committee to support the clause.

I thank the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East and the right hon. Member for Dundee East for tabling their amendment. It proposes amending one of the conditions for imposing an STPIM by changing the wording from the Secretary of State “reasonably believes” to “believes on the balance of probabilities”.

I reassure the hon. Gentleman and the right hon. Gentleman that in the development of the measures consideration was given to the conditions that must be met in such cases. The Government consider reasonable belief of a person’s involvement in foreign power threat activity to be the appropriate test for STPIMs. Foreign state intelligence operatives are highly trained, sophisticated and equipped to obfuscate in relation to their activities and avoid Government security measures. Given that, it is important that the threshold is not too high.

**Stuart C. McDonald:** The Minister appears to be saying that the test is slightly different from the balance of probabilities, but from Jonathan Hall’s evidence, he seemed to think they were pretty much the same. I want to tease out whether the Minister thinks that this test is essentially the same as the balance of probabilities, but with a slightly different formulation, or is it a lower test?

**Stephen McPartland:** I am going to give in to the hon. Member and say I think that the standard of the balance of probabilities test is slightly higher than reasonable belief, but we are dealing with incredibly sophisticated actors who are very highly trained. In this country, reasonable belief is used throughout in relation to war, and we have gone with the reasonable belief definition because of the nature of the people we are dealing with, the nature of the threats to national security and the nature of state threats, but I accept the point the hon. Gentleman is making.

**Stewart Hosie:** If the Minister is saying that the “reasonably believes” test in conditions A, C and D is appropriate for the reasons he has just given, why is condition B so hard and fast? The Bill states:

“Condition B is that some or all of the foreign power threat activity in which the individual is or has been involved is new foreign power threat activity.”

There is no evidential test, such as the Secretary of State having a reasonable belief about some or all of the foreign power activity. What is the rationale for having the slightly reduced test in conditions A, C and D, but no test at all in condition B?

**Stephen McPartland:** As I am a kind and forgiving person, I will answer and say that we have condition B because, throughout the legislation, someone has to have engaged in activity on behalf or in support of a foreign power. That is one of the key tests throughout the Bill, the foreign power test. That is the reason for it.

My view is that “reasonable belief” strikes the right balance, and the threshold mirrors that of TPIMs, which have recently been amended by Parliament in the Counter-Terrorism and Sentencing Act 2021. I ask the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East to withdraw the amendment.

**Stuart C. McDonald:** I am grateful to the Minister for answering the question. We will give that answer further thought before consideration on Report, but in the meantime, I beg to ask leave to withdraw the amendment.

*Amendment, by leave, withdrawn.*

*Clause 33 ordered to stand part of the Bill.*

### Clause 34

#### FIVE YEAR LIMIT FOR PART 2 NOTICES

**Stuart C. McDonald:** I beg to move amendment 56, in clause 34, page 25, line 12, leave out “four” and insert “two”.

*This amendment would mean the Secretary of State could seek to extend a part 2 notice on two occasions rather than four.*

**The Chair:** With this it will be convenient to consider clause stand part.

**Stuart C. McDonald:** The clause allows part 2 notices, or STPIMs, to be extended by a year. Not only that but, as drafted, the clause allows for up to four further extensions, thus allowing an STPIM to be in place for five years, even if there has been no new foreign power threat activity.

As we know, these measures can place really significant restrictions on people’s liberty. The ability to extend TPIMs was controversial and only happened after they had been in place for a significant period. The views of the previous Independent Reviewer of Terrorism Legislation, Lord Carlile QC, have been summarised as:

“The TPIM Act 2011 was a balance between on the one hand enabling administrative controls to be imposed outside the criminal process for a significant period of time, and on the other hand ensuring that individuals were not controlled indefinitely on the basis of an assessment that they had once engaged in terrorism-related activity, unless there was evidence that they have done some further act.”

Indeed, the stated purpose of TPIMs when introduced by the 2011 Act was that they were

“targeted, temporary measures and not to be used ‘simply as a means of parking difficult cases indefinitely’”.

The case for and against lifting the two-year cap was considered in detail by another independent reviewer, Lord Anderson, in his report, “Terrorism Prevention and Investigation Measures in 2012”. He observed that it was tempting to wish for longer in the most serious cases, noting:

“The allegations against some subjects are at the highest end of seriousness”.

However, he concluded that the two-year limit was an “acceptable compromise” because, in summary,

“even 2 years was a serious length of time in the life of an individual, and TPIMs should not be allowed to become a shadow alternative to criminal prosecution with their lesser standard of proof...with the possibility of no serious thought being given to how the measures might come to an end.”

It is easy for the Government to say, “Let’s mirror the current TPIM time limit as it is now,” but why should we do that? Those time limits were extended to five years only after about a decade of use of TPIMs. Starting with a five-year time limit appears to be jumping off at the deep end. If we want to mirror TPIMs, we should start off with a much shorter time limit, as happened with TPIMs, and then if, over time, evidence shows that a longer limit is required, we can make that change. But it should be based on evidence about how the orders are operating in practice and not just on saying, “Let’s cut and paste the existing position with TPIMs.”

**Holly Lynch:** I thank the hon. Member for Cumbernauld, Kilsyth and—

**The Chair:** Kirkintilloch.

**Holly Lynch:** Kirkintilloch East. Thank you for that, Mr Gray—make sure that is in *Hansard*.

I thank the hon. Member for amendment 56. Clause 34 stipulates that a part 2 notice can remain in force for a limit of five years. There are a number of overlapping clauses in this part of the Bill, focusing on reviews and the ongoing considerations about the necessity of a TPIM. When we get to clauses 39 and 40, I will speak to the importance of the TPIM review group, which Jonathan Hall made very clear in his evidence is essential if we are to learn anything from the lessons of TPIMs. On clause 34, could the Minister confirm the due regard that the Secretary of State must have for other agencies and the review group when considering whether to extend a part 2 notice?

**Stephen McPartland:** I will start with the clause and then deal with the amendment. Clause 34 provides for when a STPIM notice comes into force, how long it will remain in force and how many times it can be extended. It sets a five-year limit in total. Once a notice has been imposed, it remains in force for one year. Unless renewed, it will expire after that time.

If the Secretary of State believes that conditions A, C and D, which we have just discussed, are met, it may be extended for a further year up to four times, taking the total to five years. A further STPIM notice cannot be imposed after this time unless new foreign power threat-related activity is uncovered. I would also like to make it clear that the notice is reviewed every quarter. Those measures ensure that STPIMs cannot be imposed indefinitely, and there are constant safeguards throughout their imposition.

The one-year period and the five-year limit balance the need to protect against threats to the UK from individuals, and allow further extensions to be granted if there continues to be evidence of the risk of involvement in foreign power threat activity. The provisions do not just look back, but recognise the important work that our security services and police would need to carry out both before and after a notice expires. I would therefore appreciate the Committee’s support for the clause.

Amendment 56 relates to the time limits placed on part 2 notices. Like hon. Members, the Government agree that it is important to ensure that individuals are not placed on STPIMs indefinitely. That is why we have

[*Stephen McPartland*]

included two important time-limit safeguards. The first is that STPIMs can be extended only after a year if the conditions on which they were imposed are still met. In particular, the approach we have taken contains a number of points where positive action is required to keep an STPIM in place. That important safeguard ensures that an STPIM cannot remain in force when it is no longer appropriate.

Secondly, STPIMs can be extended on only four occasions. The hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East asked why we had not opted for two occasions, mirroring the original TPIM legislation. That is because of evidence over the last decade from our operational partners about what they feel is appropriate and necessary. We are mirroring their experience with TPIM notices over the last decade, and we will work with them on STPIM notices.

The one-year period and the five-year limit balance the need to protect against further threats. Given the safeguards I have outlined, I ask the hon. Member to consider withdrawing his amendment.

**Stuart C. McDonald:** I am grateful to the Minister, because he did not just say, “Well, we’re just cutting and pasting from TPIMs.” He did provide an explanation of the thinking behind the five-year limit. I will take that away and give it further thought. In the meantime, I beg to ask leave to withdraw the amendment.

*Amendment, by leave, withdrawn.*

*Clause 34 ordered to stand part of the Bill.*

*Ordered,* That further consideration be now adjourned.  
—(*Scott Mann.*)

10.32 am

*Adjourned till this day at Two o'clock.*



