This evidence includes content that some may find distressing [SCS0045]

Written evidence submitted by the Parliamentary Security Department

Written Evidence to the Speakers' Conference on the Harassment and Intimidation of Members (2025)

Vulnerability Reduction

1. On 15 October 2021 Sir David Amess MP was murdered by a terrorist. The following week, the Speaker of the House of Commons and the Home Secretary jointly commissioned a review of the existing security measures for MPs. The review's recommendations were accepted by the Speaker and Home Secretary in April 2022.

2. Since the implementation of RoMPS, PSD has continued to review security measures to ensure they remain effective against the evolving threat landscape. Recent innovations include pilots software which cleanses Members' feeds of abusive posts. Whilst PSD always looks to improve the offer and delivery of security measures to MPs, we are nearing the point where a further step change in vulnerability reduction measures would be neither desirable (in terms of democratic engagement) nor deliverable (in terms of available private sector security operative resource). Given that security risk is a combination of threat and the vulnerability of an individual to it, this underscores the importance of work to reduce the threat.

3. The responsibility for threat reduction sits with the Police, Crown Prosecution Service (CPS) and courts, who together identify, investigate and bring to justice those who commit offences against MPs. We aspire to work with the Police and other partners to more comprehensively understand the nature of offending against MPs, identify and address bottlenecks in the criminal justice system, build specific capabilities required to combat the specific crimes most committed against MPs, and create a stronger 'centre' to identify and coordinate policing responses to problematic offenders at a national level.

General Election

4. Ahead of the General Election, anticipating a high turnover of MPs (and thus a high level of demand for security measures and services), PSD worked with our contractors to scale up capacity of measures and services. One recruited an additional 200 close protection operatives (CPOs) and confirmed access to accredited sub-contractors to provide additional resilience. Another trained and vetted an additional 20 surveyors for the Parliamentary contract, whilst increasing surge capacity across installation teams and sub-contractors; in addition 2 full time employees joined their Helpdesk Team to increase capacity. We also expanded our own cohort of 'local security advisors' (LSAs) from 4 to 9 in time for the election, to ensure national coverage for the incoming cohort of MPs.

5. Parliament cannot provide personal security protection to candidates during Dissolution (due to concerns about conferring an advantage to the incumbent). Therefore PSD worked with the Police and Home Office to ensure that Home Office close protection provision and established risk assessment processes continued to operate seamlessly throughout Dissolution and into the new Parliament.

6. In July 2024, 350 new Members were elected to Parliament, a significant churn.

7. In response, PSD worked quickly to enhance the capacity and capability of private contractors responsible for delivering security measures ahead of the election, and have focused on installing the

main three electronic security measures for new MPs at their constituency homes as a priority since July 2024 (following up with new MPs' offices as these began to be acquired from Autumn 2024 onwards).

8. New Members have been enthusiastic users of close protection operatives. We are working with our contractor to ensure that we maximise capacity and are clearer with MPs about the circumstances in which the use of security operatives are recommended.

Social Media: Abuse, Intimidation and Threats

9. Since 2021, PSD has, on behalf of MPs, sought to identify publicly viewable social media messages which abuse, intimidate or threaten them. PSD will refer potentially criminal material to the Police for assessment, and potential breaches of social media terms of service to platforms for potential action.

10. Over the years, the amount, intensity and nature of abusive, intimidating and threatening material on social media platforms has increased, whilst the willingness of some platforms to remove such material has diminished. A general move from US-headquartered social media companies to prioritise freedom of speech over moderation of abusive and intimidatory material has only gathered pace in recent times, and is not likely to reverse under the current American political administration. With business models which rely maximising user numbers and regular controversy drawing in advertising revenue, there is minimal incentive for platforms to remove content or sanction users for content which is 'lawful but awful' in nature.

Examples of social media messages directed towards MPs deemed **not** to be in violation of the platform's terms and conditions:

"*My friend says you look like an orc my nigga, now go back to Africa, you are trash occupying foreign lands*"

"*Islam has encouraged the full destruction of everything else for 1400 years. You should write a letter about how the vile Muslim cancer should be exterminated."*

"You are a despicable, gaslighting rodent who needs lining up against a wall with the rest of your verminous ilk."

"You're a shit human being belonging to a shit religion that worships death."

"Fucking slapper."

"The gross dyke haircut tells you all you need to know."

11. These are a tiny fraction of the unsuccessful referrals PSD has made over the years.

12. PSD has twice changed its thresholds for referring messages to social media platforms due to the high proportion of abusive messages not being taken down. We now routinely refer only directly threatening and grossly offensive material to platform, as we know this is the only material that will be considered for removal. Whilst this means the percentage of content actioned as the result of a referral from PSD has recovered from a low at the end of 2022, far fewer posts are identified and actioned than would have been the case three years ago.

This evidence includes content that some may find distressing [SCS0045]

The Nature of Security Incidents Faced by MPs

13. In late 2024 PSD and the Metropolitan Police introduced a new, comprehensive system for categorising security incidents logged by Police nationwide[1] in relation to MPs. Whilst it has always been possible to track specific crimes committed against MPs (as they are defined in law and consistently understood across Policing), the new system (the Operation BRIDGER 'taxonomy') has for the first time allowed PSD and the Police to categorise and quantify incidents not reaching the criminal threshold, but crucial for understanding the threat to MPs.

14. The taxonomy now records the type of incident, the nature of the contact between the perpetrator and the MP, and the motivation of the perpetrator, where it is known or can be reasonably suspected. Analysis of data from October-December 2024 suggests:

- The vast majority of security incidents, both criminal and non-criminal, are conducted via 'virtual means;' by email, social media, telephone or letter (83% during this period). Only a small proportion of incidents (12% this period) happen face to face with the MP or their staff.[2]

- The majority of 'virtual' incidents are abusive, threatening, intimidating or concerning/critical emails; most of the rest relate to social media messages.

- Where incidents took place 'in person,' over half took place at the MP's constituency office or surgery. Only a very small proportion of 'in person' incidents took place at an MP's home and related to a variety of issues, including unwelcome approaches and the delivery of a suspicious parcel.

- Linked to the above, the most frequent crime recorded as committed against MPs is that of Malicious Communications (45% in this period),[3] followed by Harassment (23%).

- Similarly, the most common non-criminal incidents logged by the Police are abusive and threating communications (mostly emails and social media messages).

- For the majority of security incidents, the motivation of the perpetrator cannot be immediately determined (as the abuse/complaint/threat is too general and the perpetrator, at least initially, unidentified).

- Where the perpetrator's motivations can be determined or reasonably suspected, the majority of incidents are related to political grievances, either driven by animus against a particular Party or Member, or relating to a particular topical political or societal issue (assisted dying, winter fuel payments, grooming gangs, etc).

---

[1] On the Police's national 'Mercury' database, which records such incidents.

[2] Incident rates when compared with relative representation in Parliament are suggestive but not conclusive; 40% of MPs are female; 49% of Malicious Communications and 53% of non-crime abusive, intimidating and threatening incidents are directed against female MPs, so 'abuse' of female MPs does seem to be more prevalent.

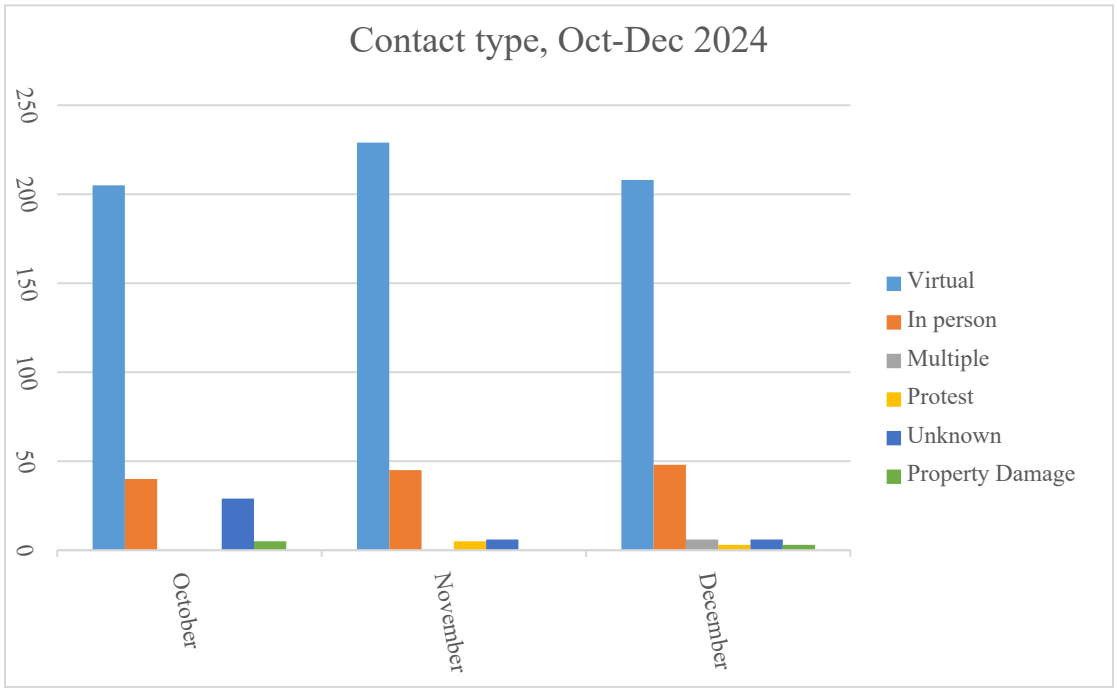
[3] Governed by the Malicious Communications Act (1998) and Communication Act (2003) and pertaining to 'grossly offensive' communications.

- Racial abuse and offensive/rambling/incoherent messages driven by suspected mental health issues are also both significant subsets of those incidents where the perpetrator's motivation is known.

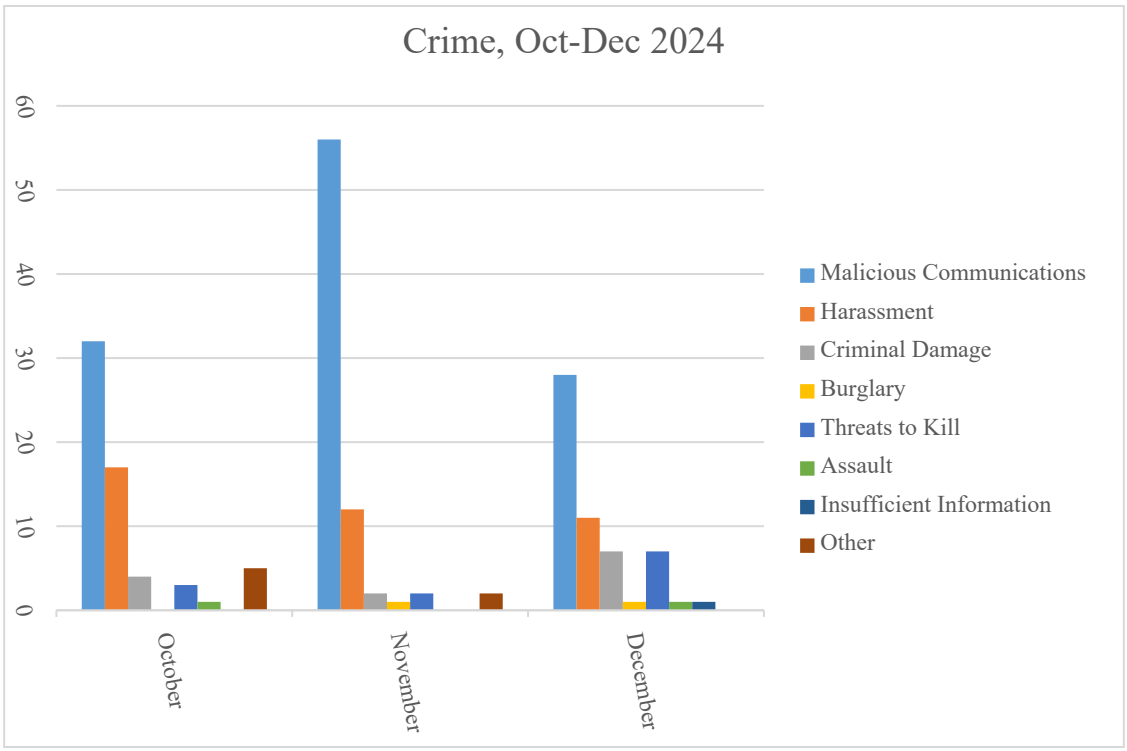
- It is surprising that misogynistic abuse is not as prevalent as racial or religious abuse, given what we know about social media and the nature of abuse in general; we are working to ensure we have a clear understanding of what is deemed to be misogynistic in nature to ensure we are not underreporting this type of incident.

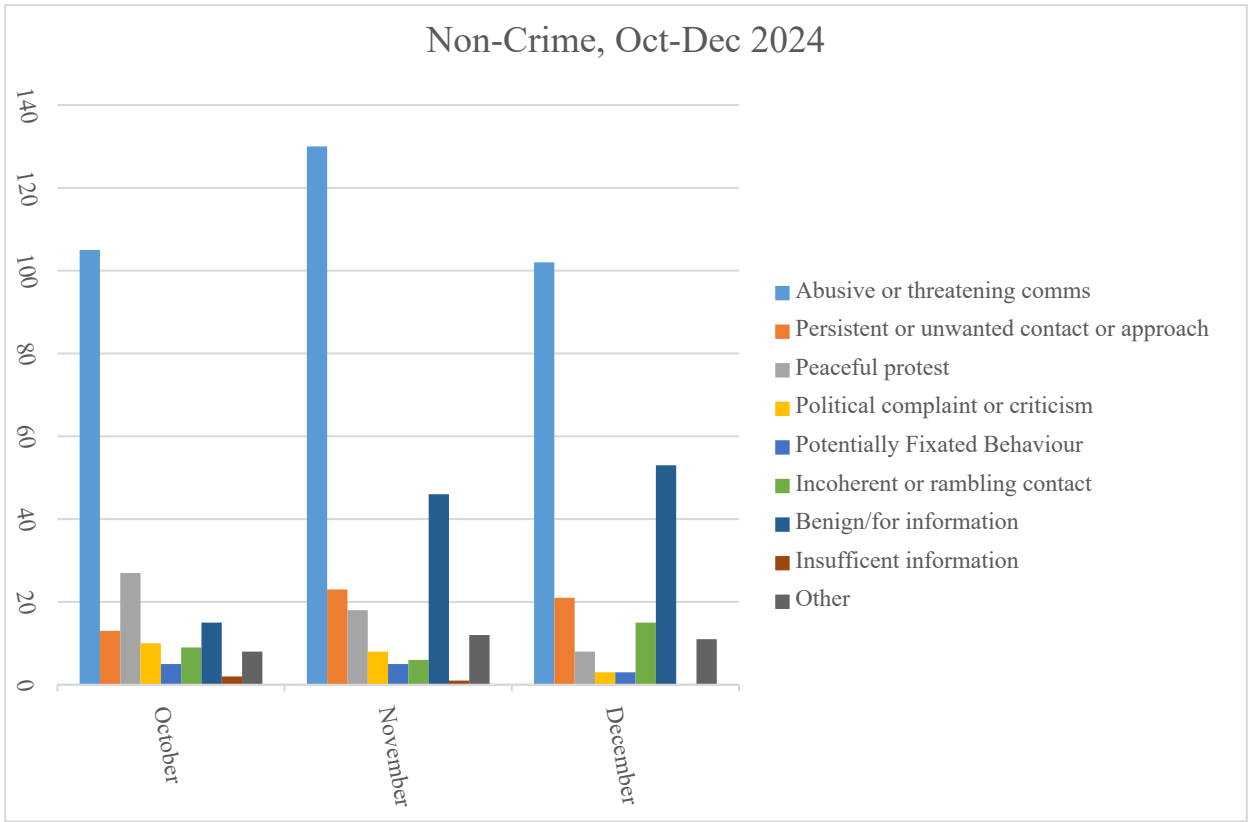
15. It should be noted that this data only reflects incidents known by or reported to the Police, although the volume of existing reporting suggests that the trends outlined above are broadly reflective of incidents suffered by all MPs.

Taxonomy Data Charts



This evidence includes content that some may find distressing [SCS0045]





This evidence includes content that some may find distressing [SCS0045]

March 2025