Written Evidence pertaining to draft sections 148 and 149 (direct and indirect disclosures: no breach of obligation of confidence) of the Economic Crime and Corporate Transparency Bill 2022 from the Royal United Services Institute for Defence and Security Studies (RUSI)

1. This submission is made by the Centre for Financial Crime and Security Studies (CFCS) at the Royal United Services Institute (RUSI). Since its formation in 2014, CFCS has focused on matters at the intersection of finance and security in support of policy makers and operational agencies in the UK and in a range of countries across the globe. Queries about this submission should be forwarded to the CFCS Programme Manager, Alanna Putze.
2. This submission represents the views of the research team members who have contributed their expertise. It does not represent the views of RUSI itself.
3. Further evidence on global best practices in private-private information-sharing will be submitted by the RUSI partner programme Future of Financial Intelligence Sharing (FFIS) in a separate submission.

Information-sharing: Global Best Practices

4. As the international standard-setter for anti-money laundering (AML) and counter terrorist financing (CTF), the Financial Action Taskforce (FATF) notes *"effective information sharing is one of the cornerstones of a well-functioning AML/CFT framework".* According to FATF *"barriers to information sharing may negatively impact the effectiveness of AML/CFT efforts and conversely, inadvertently facilitate operations of such criminal networks.".* [1] Our own research in this field notes that fighting economic crime without data-sharing *is "like trying to complete a jigsaw puzzle without knowing who has the next missing piece"*[2].
5. On this basis the stated aim of the provisions in the Bill - to give the private sector *"more confidence to share information in order to tackle money laundering and other economic crime"* is the right one. The draft provisions contained in the Bill are certainly welcome and will enable 'regulated sector' businesses to share individual pieces of information in specified circumstances to prevent criminals from exploiting the information gap between regulated institutions in cases where, for example, a decision has been made to exit a client relationship due to money-laundering concerns.
6. However, these provisions, while welcome, fall short of achieving the UK government's stated ambition, as set out in the Economic Crime Plan 2019-2022, to *"establish the UK as a world-leader in promoting the appropriate and proportionate sharing and use of high-quality information for economic crime purposes"*[3].
7. While the provisions are a necessary step forward and remove *one* of the barriers to greater information-sharing between private sector entities, they do not provide the basis for the UK to keep pace with international best practices, which are moving beyond small-scale, analogue information-sharing into large-scale, technologically-enabled collaborative analytics, supported by privacy preserving technologies.
8. In FATF's July 2022 guidance on private sector information-sharing[4] it notes the benefits of larger-scale data-sharing, in appropriate circumstances. It notes that *"by using collaborative analytics, bringing data together, or developing other sharing initiatives in responsible ways, financial institutions seek to build a clearer picture of the puzzle, to better understand, assess, and mitigate money laundering and terrorist financing risks."*

[1] "FATF Guidance: Private Sector Information Sharing", November 2017, pg 2.
[2] "Enabling Cross-sector Data-Sharing to Better Prevent and Detect Scams", Westmore et al, RUSI, October 2022.
[3] UK Economic Crime Plan (2019-2022), para 3.13.
[4] "Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information-Sharing", FATF, July 2022.

9. FATF, in its support for greater moves towards data pooling and collaborative analytics, notes that *"where one institution might struggle to identify a complex suspicious transaction pattern or network, information from other institutions may complete this picture"*.
10. While a nascent development in global anti-financial crime, the trajectory of travel globally is towards supporting private sector entities in establishing shared collaborative analytic platforms, using appropriate legal and technological safeguards to uphold privacy. In its 2022 guidance, FATF notes that governments should support such efforts through legislative and regulatory change.
11. It is notable that a limited number of jurisdictions are already some way down the line in their journey towards greater, at scale, data sharing. Below are some specific examples of nascent shared platforms currently under development in the Netherlands and Singapore.

Netherlands: Transaction Monitoring NL (TMNL)

12. In the Netherlands, five financial institutions have signed an agreement, endorsed by the Dutch government, to establish a joint transaction monitoring shared utility – Transaction Monitoring NL – to allow for the sharing of transaction monitoring alerts to prevent layering of money-laundering through multiple banks. The platform will utilise pseudonymised data (to protect the underlying personal data) which can only be unlocked if a match is made.
13. In the first instance data will only relate to corporate entities. However, legislation is currently under debate in the Dutch Parliament to support the sharing of personal data, with appropriate oversight and protections. To support financial institutions in sharing this information, the draft legislation currently *mandates* the sharing of information in order to overcome barriers (real or perceived) within data protection legislation.

Singapore: COSMIC Platform

14. The Monetary Authority of Singapore is currently consulting on the establishment of a new government-led digital platform to support greater private-private sharing of information for the purposes of tackling money-laundering (the Collaborative Sharing of Information for ML/TF Cases or COSMIC platform).
15. Although currently still under consultation, the draft law underpinning the new platform, like that in Holland, envisages mandated information-sharing through the platform *as well as* removing the civil liabilities surrounding duty of confidence.

Conclusion

16. In summary, while the amendments contained in sections 148 and 149 of the proposed legislation are necessary, they do not keep pace with international best practice. It is essential that the government's forthcoming second Economic Crime Plan (due for publication in early 2023) sets out a more ambitious vision.
17. Whether the approach of mandating information-sharing under shared platforms (as the approaches in the Netherlands and Singapore currently suggest) is the right one for the UK, however, requires considerable debate given the necessary tensions between economic crime and data privacy policy goals.
18. Whatever the result, it is important that future information-sharing reforms do not operate within a policy silo and that the government considers how economic crime information-sharing can be supported through reforms within the broader data protection landscape (including within the Data and Digital Information Bill) and through regulatory guidance from both AML supervisors and the Information Commissioner's Office.
19. In addition, future reforms must tackle the cultural and behavioural barriers which prevent organisations from willingly sharing data. While the current legal and regulatory framework allows data-sharing for the purposes of economic crime prevention, organisations and stakeholders within an organisation have very different risk appetites. There is an opportunity with future legislation and regulation to make a clearer statement of intent about the extent to which organisations should share data and to use language which creates an environment that is more permissive to responsible data-sharing.