ASIC
Australian Securities & Investments Commission

# ASIC's position on the Department of Communications submission to the Inquiry into s313(3) of the *Telecommunications Act 1997*

We understand that the Committee is interested in ASIC's views on the Department of Communications' proposed whole-of-government guidelines which would specify minimum requirements for agencies that use s313 to request the disruption of access to online services. The Department of Communications' proposed requirements, and our position on each requirement, are set out in the table below.

| Department of Communications proposed requirements | ASIC position |
|---|---|
| 1. Develop agency-specific internal policies outlining their own procedures for requesting the disruption of access to online services (recognising that agencies will have different requirements based on their operational activities). | Agree.<br>Our submission notes that the Committee may wish to consider the measures raised by the Department of Communications – including that agencies should develop clear blocking policies.<br>(see ASIC submission page 8) |
| 2. Seek clearance from their agency head (or Minister) prior to implementing a service disruption policy for illegal online services as part of their operational activities.<br><br>The approval should set out who in the agency (level of officer) is authorised to make subsequent requests under s313 to disrupt access to services. | Agree.<br>Our submission notes ASIC's current approach to applying for stored communications as an example. That is, the ASIC Chairman has nominated a member of the Commission, Regional Commissioners, and SELs to make applications for stored communications warrants.<br>(see ASIC submission page 6) |
| 3. Ensure that disruption of services is limited to specific material that draws a specified penalty (for example, a maximum prison term of at least two years, or financial equivalent). | Agree.<br>Our submission also highlights the importance of capturing investment fraud in any definition.<br>(see ASIC submission pages 6 – 7) |
| 4. Consult across government and relevant stakeholders (such as ISPs) to ensure that the technical measures outlined in their services disruption policies are effective, responsible and appropriate. | Agree. We note this proposed requirement.<br>(see ASIC submission page 8) |
| 5. Use stop pages where operational circumstances allow, and include, where appropriate:<br>• the agency requesting the block;<br>• the reason, at a high level, that the block has been requested;<br>• an agency contact point for more information; and<br>• how to seek a review of the decision. | Agree. We note this proposed requirement.<br>(see ASIC submission page 9) |
| 6. Publicly announce, through means such as media releases or agency website announcements, each instance of requesting the disruption of access, where doing so does not jeopardise ongoing investigations or other law enforcement or national security concerns | Agree. We note this proposed requirement.<br>(see ASIC submission page 9) |
| 7. Have internal review processes in place to quickly review a block, and potentially lift one, in cases where there is an appeal against the block; | Agree. We note this proposed requirement.<br>(see ASIC submission page 9) |
| 8. Report blocking activity to the ACMA, or where operational circumstances make this impossible or impractical, to the appropriate Parliamentary Committee. | Agree. We note this proposed requirement.<br>(see ASIC submission page 9) |