Australian Government

Government Response to the Independent Review of the *Online Safety Act 2021*

14 April 2026

Preamble

This is the Australian Government's response to the Report of the Statutory Review of the *Online Safety Act 2021* conducted by Ms Delia Rickard PSM. The review was a comprehensive examination of the Act to ensure Australia's online safety laws remain fit for purpose in an ever-changing online environment.

The Government thanks Ms Rickard for undertaking this important review and acknowledges the broad community consultation that has informed the review's 67 recommendations. The Government extends its gratitude to the many individuals and organisations who contributed their insights, experiences and expertise to support positive online experiences for the Australian community.

Australia's world-leading *Online Safety Act 2021* (the Act) sets the benchmark for addressing online harms to individuals and holding industry to account for the safety of their services. Much has been achieved since the Act came into effect. The Act has provided pathways to help individuals impacted by harms online, facilitated the removal of unlawful and restricted material, and improved the overall safety of user experiences and online regulation standards. However, the technology and services within scope of the Act continue to evolve at a rapid pace. The Government is committed to ensuring our laws continue to provide the right protections and that our online safety regulation remains effective.

The Government recognises the significant challenges industry and regulators face in protecting users online. As the conduits for access to the online environment, digital service providers have a unique and important role to play in supporting safer online experiences.

The review made 67 recommendations to Government, focussing on better protections for Australians from online harm, including recommendations for more systems-based approaches, better support for individuals and ways to make sure the online regulator has the tools needed to do its job.

Building upon the Government's existing commitment to introduce a duty of care in the Online Safety Act, the Government intends to implement, wholly or partially, or further consider 64 of the 67 recommendations. The Government's position on each recommendation of the review's 67 recommendations is outlined below. As an immediate priority, the Government has committed to reforms that incentivise harm prevention, including implementing a digital duty of care, and other reforms that address the operational challenges and limitations of the Act.

Legislating a digital duty of care, a key recommendation of the review, will place obligations on service providers to proactively and effectively manage the risk of harms from the use and misuse of their platforms and services – something that they are best placed to do. In

line with the Government's response to the recommendations of the review outlined below, additional amendments to the Act will be made to ensure the duty of care creates an effective, simplified framework which operates coherently with related initiatives, including proposed reforms to Australia's privacy laws. The Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts is leading this work and a bill will be introduced, consistent with the Government's legislation priorities.

Government Positions on the Recommendations of the Review

The Government's response to each recommendation is listed below and includes the following responses:

- **Support**, where all elements of the recommendation are supported.
- **Support in principle**, where the Government generally supports the intent or merit of the recommendation but considers that there are other more effective ways to deliver on this intent or where further consideration is required to consider implementation, resourcing and prioritisation options.
- **Note**, where further analysis is required for the Government to determine its position
- **Not supported**, where the Government does not support the recommendation.

A duty of care on services to keep Australians safe online

A duty of care will support broad, risk-based and proportionate regulation of all digital service providers and provide a legislative framework that can better accommodate changes in technology and services (recommendations 4, 6, 8, 11, 12).

The Act will be amended to include a statutory obligation for service providers to take reasonable steps and exercise due diligence in maintaining their systems and processes to prevent harm resulting from the use of their service.

The Government acknowledges the benefits of more descriptive objects in the Act to provide greater clarity. Existing definitions will be maintained, with further work to determine necessary amendments to improve their operation (recommendations 1, 2).

The Government will determine whether opportunities exist to develop policies or guidance to recognise and support providers of online safety-related services and technology (recommendation 3).

The Government supports a focus on protecting vulnerable Australians including children, combating criminal activity and promoting public safety, while also respecting Australians' freedom of expression. The duty of care will complement criminal offences in the *Criminal Code Act 1995*, and does not alter existing legal obligations under other legislation, including the *Racial Discrimination Act 1975*, *Sex Discrimination Act 1984*, *Disability Discrimination Act 1992* or the *Age Discrimination Act 2004* (recommendation 5).

The duty of care will be risk-based and proportionate and applicable to all service providers where there is a risk of harm to Australians. High or fixed thresholds are therefore not required to be determined (recommendation 7).

The duty of care may be supported by rules made by Government and these rules will be subject to Parliament scrutiny (recommendation 9).

Broad transparency reporting powers under the Basic Online Safety Expectations (BOSE) will be retained (recommendation 10).

The Government supports the intent of the review to improve the transparency of digital services by supporting the important work that expert researchers perform (recommendation 13).

Review Recommendation	**Government Response**
01: That the objects of the Act should be amended to include more descriptive objectives that are linked to the various functions covered by the Act.	Support
02: That current definitions of the online industry sections should be simplified to online platforms, online search and app distribution services, online infrastructure services and equipment and operating system services. These should be included in the Act to better reflect online safety risks and future proof the Act.	Note
03: That the Government consider options to recognise the role of providers of online safety related services and technology in helping to identify and stop the distribution of child sexual exploitation and abuse material.	Support in principle
04: That Australia adopt a singular and overarching duty of care that encompasses due diligence, and is underpinned by safety by design principles, risk assessment, risk mitigation and measurement.	Support
05: The harms that should be highlighted for attention under a duty of care should at a minimum include: • Harms to young people, including child sexual exploitation and abuse (including grooming), bullying and problematic internet use • Harms to mental and physical wellbeing, including threats to harm or kill, or attacks based on a person or group of people's protected characteristics, such as sex, gender, sexual orientation, race, ethnicity, disability, age or religion • Instruction or promotion of harmful practices, such as self-harm/suicide, disordered eating and dares that could lead to grievous harm	Support in principle

• Threats to national security and social cohesion, such as through promotion of terrorism and abhorrent violent extremist content; and • Other illegal content, conduct and activity.	
06: Entities with the greatest reach or risk should be required to complete a risk assessment at least every 12 months and to carry out a risk assessment when significant changes are made to the design and operation of their service. These entities should also be required to provide an annual report detailing their risk assessments, risk mitigations and how successful they have been to the regulator.	Support in principle
07: Services used by more than 10 per cent of the Australian population should be automatically part of the highest tier with additional mandatory responsibilities. The regulator should have a power to deem whether other online services do, or do not, meet the reach or risk requirement, noting that the reach or risk of services may change over time.	Not supported
08: The best interests of the child should be a primary consideration for online service providers in assessing and mitigating the risks arising from the design and operation of their services, including risks to children who may use the service and risks to children as a result of how the service may be used.	Support
09: The eSafety Commissioner should be empowered to create mandatory rules (in the form of codes) on how entities can comply with certain aspects of the duty of care requirements, including addressing specific online harms. This should not stop services from taking additional steps to protect people. Codes would not create safe harbours.	Support in principle
10: In addition to risk assessments, a service with the greatest reach or risk should be required to provide an annual transparency report and publish a summarised version on its website. This should not replace the broad power for eSafety to require periodic and non-periodic transparency reports from all services.	Support in principle
11: Services with the greatest reach or risk should be required to have a well-resourced compliance function that reports directly to senior management as needed, and at least quarterly	Support in principle

to the audit and risk committee and annually to the board. Only the board (or its equivalent) can dismiss the head of the compliance function.	
12: The regulator should have the discretion and power to require services to undertake an audit at their own expense.	Support
13: Subject to adequate safeguards, services with the greatest reach or risk should be required to share data with authorised researchers for the purposes of determining compliance with a duty of care model, the takedown schemes and research into emerging problems and harms.	Support in principle

Supporting people who have experienced harms online

The Government remains committed to supporting Australians who have been harmed online and is focused on delivering practical and effective reforms that provide obvious and attainable benefits to Australians.

The process for eSafety to issue removal notices will be streamlined to enable a rapid response to a recurring harm which has already been subject to a removal notice (recommendations 15, 16, 19).

Recommendations 18, 20 and 21 require further consideration as these suggest a response to individual incidents and/or users, rather than the systemic approach of the duty of care.

While lowering the threshold of the Adult Cyber Abuse Scheme would appear to provide greater support to Australians who experience online harm, it is likely that expanding this Scheme would be operationally burdensome and counterproductive. A key goal is finding the balance between the future focus of harms prevention through a systemic duty of care and reforms to the Act to strengthen reactive powers.

Defining 'reasonably proximate cumulative harm' would be challenging as it is an inherently subjective concept dependent on context and personal interpretation of harm. Integrating this into the Adult Cyber Abuse Scheme would be complex and require significant resources which may not deliver the intended outcomes. Capturing the intent of this recommendation will be considered in the development of the duty of care (recommendation 22).

Options that contribute to addressing volumetric attacks will be considered in the development of the duty of care. The issue is complex, layered and continually evolving and developing an appropriate definition that will stand the test of time will need to be carefully tested with stakeholders (recommendations 23, 24).

Several reforms identified in the report, including informal take down, 'no wrong door', and fusion cells to address wicked problems, will be explored further, including investigating options to address the proposals (taking into account the need to ensure regulator efficiency) through non-regulatory means (recommendations 14, 17, 28).

The Government is committed to ensuring Australians have access to appropriate pathways to resolve issues they face online. Current complaint schemes will be retained, with the Act amended to provide the eSafety Commissioner the power to require service providers to have accessible and simple ways for users and non-account holders to make complaints about online content or platform features (recommendation 25).

The Government will initially focus on improving support for Australians online by promoting improved internal dispute resolution mechanisms for online services (recommendation 26).

On 2 September 2025, the Government committed to working with industry to consider how to restrict access to nudify services and undetectable stalking apps. This work is continuing, including through the duty of care framework which will place an obligation on services to put in place systems and process to prevent their services being used to cause harm. In addition, new bespoke powers that allow the regulator to issue notices to remove nudify apps and websites will be introduced (recommendation 27).

Review Recommendation	**Government Response**
14: For the avoidance of doubt, the legislation should make it clear that informal requests for takedown are legal and legitimate as they lead to quicker results for individuals who are often in severe distress.	Support in principle
15: Users experiencing adult cyber abuse or child cyberbullying should only need to wait 24 hours (not 48 hours) following a complaint to a service before eSafety is able to issue a removal notice.	Support
16: The regulator should be empowered to waive the statutory delay to issue a removal notice for the child cyberbullying and adult cyber abuse schemes where no clear complaint mechanism exists on the online service, or where reporting would lead to a reasonably foreseeable risk of further harm to the user experiencing the abuse.	Support
17: The Government should develop a whole of government 'no wrong door' approach to support individuals seeking help to address online harms. This will require cooperation and information sharing across portfolios, including law enforcement, to address a range of issues such as online safety, child safety, privacy and scams, among others.	Support in principle

18: The adult cyber abuse scheme should be amended by lowering the threshold. The new threshold should require that an ordinary reasonable person would conclude that 'it is likely the material was intended to have an effect on a particular Australian adult', and that an ordinary reasonable person would 'regard the material as being, in all the circumstances, menacing, harassing or seriously offensive.	Note
19: The Act should enable the regulator to issue a removal notice for material that has met the regulatory threshold for removal under a prior complaint, where the regulator becomes aware that the material has been reposted.	Support
20: The Act should include additional powers to require an end-user to stop posting cyber abuse about an Australian adult in an end-user notice, subject to a civil penalty for non-compliance.	Note
21: The Act should include a definition of online hate material. The definition should acknowledge that online hate involves an attack against a person or people that is based on a protected characteristic and can include dehumanisation. Notably, the definition of online hate material should not include views regarding ideas, concepts or institutions. The definition should also consider potential exclusions (for example where material is posted for artistic, scientific, or journalistic purposes).	Note
22: The Act should be amended to ensure that, in interpreting the threshold of harm for adult cyber abuse, the reasonably proximate cumulative harm caused by online hate material is taken into account.	Note
23: The Act should define a 'volumetric attack', and the regulator should be empowered to issue a notice or notices to multiple platforms based on a single complaint to address volumetric attacks.	Note
24: The Act should be amended to provide the regulator with the ability to issue a notice to services in relation to a suspected 'volumetric attack', which may require information related to the attack, specify remedial actions to be taken, and require the service to report back on steps taken.	Note
25: All services should be required to have an easily accessible, simple and user-friendly way to make a complaint and internal complaint handling processes that are in line with a code on internal dispute resolution. In particular, this should include a way for non-users to report issues such as when intimate images have been posted without consent on a service. Services should also be required to respond to reports within a reasonable time and for some issues within 24 hours.	Support

26: In line with the Australian Competition and Consumer Commission's Digital Platform Services Inquiry, the Government should develop and implement an Ombuds scheme that covers digital platforms and online search and app distribution services.	Note
27: The Government should explore how best to prohibit search engines and app stores from surfacing, selling or distributing 'nudify' apps and undetectable stalking apps.	Support
28: The Government and the regulator should both be able convene multi-stakeholder 'fusion cells' to analyse 'wicked problems' (such as the implications of end-to-end encryption for combatting child sexual exploitation and abuse, and technology-facilitated abuse and gender-based violence) and develop coordinated multi-stakeholder solutions.	Support in principle

Links between the OSA and the National Classification Scheme

The Stage 2 reforms to the National Classification Scheme (the Scheme) are likely to have an impact on the interoperability of the Scheme and the Act. Further consideration will be given to decoupling the Act and the Scheme following implementation of the planned reforms of the Act and the Scheme (recommendations 29, 30, 31, 32, 33).

Interim measures will be considered to address any short-term issues that impact on current operations of the eSafety Commissioner.

Review Recommendation	**Government Response**
29: The Act should be decoupled from the National Classification Scheme with new Class 1 and Class 2 definitions and thresholds specified in the Act and, as far as possible, be based on equivalent standards in the National Classification Scheme.	Note
30: New Class 1 definitions and thresholds should clearly focus on illegal and seriously harmful material and directly correspond to the Criminal Code where appropriate. Sexually explicit material that includes violent and seriously injurious practices, such as choking, should sit under Class 1.	Note
31: New Class 2 definitions and thresholds should include material that is legal but may be harmful, particularly for minors, and consensual sexually explicit material including non-injurious fetish material.	Note
32: Class 2 definitions and thresholds should also capture material dealing with harmful practices such as disordered eating, self-harm and substance use to address their heightened impact, especially on young people, in the context of social media. In the longer term, so that adults are covered, industry	Note

should be obliged to prevent dissemination of such content through a broader code dealing with mental and physical wellbeing under duty of care provisions.	
33: In reforming the Act and the National Classification Scheme, the regulatory remit of eSafety should be clarified. Content that is subject to the National Classification Scheme should fall outside eSafety's remit (except features that are uniquely social media enabled).	Note

Stronger penalties and enforcement powers

The Government recognises the importance of providing the online safety regulator with appropriate enforcement powers, and for proportionate penalties for non-compliance. Accordingly, an increase to the maximum civil penalties in the Act to a level more proportionate with the potential harm of underlying offences, will be determined, better aligning to those penalties introduced as part of the *Online Safety Amendment (Social Media Minimum Age) Act 2024* or other comparable Commonwealth legislation (recommendations 34, 35).

The eSafety Commissioner will be provided stronger enforcement powers applicable to online services, building on existing expectations in the BOSE (recommendations 36, 39).

Work will be undertaken to ensure consistent regulatory powers across existing complaint and content-based removal schemes, including for issuing link-deletion notices for complaint schemes and under the Online Content Scheme, and for removal and link-deletion notices simultaneously (recommendations 37, 38).

Further consideration will be given to the following recommendations:

- consistent end-user notice powers across the schemes to assess the impact on the rights of Australian users, including privacy and freedom of expression (recommendation 40)
- expanded access restriction powers on online services to understand the impact on Australian users and businesses, including adverse impacts on legitimate access and use of online services (recommendation 41)
- business disruption powers to determine the impact on Australian users and businesses, including any adverse impact on third parties that are legitimate and compliant business entities such as advertisers (recommendation 42)

Requiring major platforms to have a local presence for the purpose of facilitating enforcement is potentially inconsistent with Australia's international trade obligations (recommendation 43).

A licensing scheme represents a significant change to the regulatory landscape across Government (recommendation 45).

Review Recommendation	Government Response
34: The maximum civil penalty that a court can impose should be increased to the greater of 5 per cent of global annual turnover or $50 million.	Support
35: The civil penalties for non-compliance with removal notices should be increased to a maximum of $10 million for companies.	Support
36: The Act should be amended to empower the regulator to use enforceable undertakings or issue remedial directions to services in relation to all relevant penalty provisions, to seek to bring them back into compliance.	Support in principle
37: The Act should allow removal and link-deletion notices to be issued simultaneously under the Online Content Scheme.	Support
38: The Act should empower the regulator to simultaneously issue link removal notices for all harmful content under removal schemes.	Support
39: The finalised duty of care model should include scope to consider repeated non-compliance by services in removing content as evidence of non-compliance with the duty of care.	Support
40: The Act should include consistent powers across the schemes to require end-users to remove content and refrain from posting abuse in the future.	Note
41: The Government should expand access restriction powers against services for seriously harmful non-compliance.	Note
42: The Government should consider options for business disruption powers for seriously harmful non-compliance.	Note
43: The Government should consider the feasibility of requiring major platforms to have a local presence for the purpose of facilitating enforcement action.	Not supported
44: The Act should require major platforms, that is those designated under the reach or risk criteria under the duty of care requirements, to have a contact point for service in Australia.	Support
45: The Government should consider options for introducing a licensing scheme for major services as a condition for operation.	Not supported

Investigations and compliance monitoring

The details of the powers and tools to monitor and investigate suspected non-compliance with the Act, and those to obtain information necessary to conduct their investigations, will

be carefully considered, having regard to the proportionality of powers and the rights of end-users (recommendations 46, 47, 48, 49).

Technical amendments to improve the intended operation of the Act will ensure the consistent application of section 205 to Part 14 of the Act, and digital services will be required to retain records necessary and sufficient to demonstrate their compliance with the Act and the steps they have taken to comply with the Act (recommendation 50).

The Act currently contains transparency powers through the BOSE, with the eSafety Commissioner able to require service providers to report on how they are meeting these expectations, and enforceable by civil penalties. These will transition with the duty of care to ensure the continuation of oversight functions (recommendation 51).

The Government supports the regulator being able to disclose information to other agencies, authorities or authorised persons where it is appropriate and necessary to fulfill a public function, enforce the law, or protect persons. Further analysis will be done on defining the scope of 'international authorities' to whom information can be disclosed (recommendation 53).

Arrangements currently exist to ensure child sexual exploitation material is removed, with memoranda of understanding in place with the Australian Federal Police and all State and Territory law enforcement agencies, as well as with the International Association of Internet Hotlines network, assisting with the rapid removal of this material overseas. These arrangements enable enforcement agencies to maintain appropriate oversight and engagement (recommendation 54).

Review Recommendation	**Government Response**
46: The Act should be amended to empower the regulator with stronger powers in relation to investigations, including to: • Incorporate the monitoring and investigations provisions of the Regulatory Powers Act into the Act • Initiate investigations of a service's compliance with the duty of care; and • Initiate investigations into reposted material that was previously reported and taken down.	Support in principle
47: Amend the Act to provide the regulator with appropriate flexibility to conduct investigations as it thinks fit, including the use of technological tools to assist with investigations and content removal, and the use of sock-puppet accounts.	Support in principle
48: Provide additional powers to the regulator to improve its ability to obtain end-user information under Part 13, including a requirement that prevents services from informing end-users when they have received a notice under Part 13, a requirement	Support in principle

for services to collect a user's phone number as a condition for opening an account, and provide a new power to compel the preservation of accounts for investigative purposes.	
49: The Act should be amended to empower the regulator with stronger information gathering powers, including to: • Improve its ability to obtain end-user information under Part 13 of the Act; and • Set the time period for a written notice to provide evidence under Part 14 of the Act.	Support in principle
50: Section 205 of the Act should be amended to confirm that non-compliance with a requirement to give evidence includes information as requested under section 199 (and other sections in Part 14 of the Act).	Support
51: The Act should be amended to require services to inform the regulator of actions the service has taken in response to the regulator's actions and requests (including informal requests).	Note
52: The Act should be amended to require services to maintain certain records, such as measures taken to comply with obligations under the Act and any actions taken in response to the regulator's requests and risk assessments, for the purposes of eSafety's investigations.	Support
53: The Act should be amended to allow the regulator to disclose information to: • Any head of a Commonwealth agency or department • International authorities; and • Teachers, school principals, parents or guardians regarding complaints from a child about image-based abuse (as can be done for child cyberbullying).	Support in principle
54: Allow the regulator to disclose certain information to Non-Government Organisations who have an approved role in assisting the regulator with enforcement activities.	Note

Awareness raising and education in the community

Awareness raising and education of the community about online safety matters are fundamental to reducing harm, with eSafety playing an important role (recommendations 55, 56).

Resourcing for awareness campaigns and activity, including potential regulator name changes, will be considered as part of future funding for eSafety as required (recommendation 57).

Review Recommendation	Government Response
55: The regulator's continued awareness raising activities should include in-person outreach, including in hard to reach communities, and hard copy resources.	Support
56: Educational and promotional material should not only focus on what the regulator does for people experiencing harms, but also include simple messaging about how to make a complaint. Online safety education delivered at schools should focus on awareness of the regulator as a source of help. News media outlets should be encouraged to provide information about the regulator at the end of articles detailing experiences of online harms.	Support
57: If a decision to make structural changes to the regulator includes a change to its name, a major campaign re-launching the regulator should be conducted. The timing of this campaign should be coordinated to align with major changes to the Act.	Note

A stronger regulator

The Government is committed to supporting a responsive online safety regulator that can deliver for all Australians.

As the review observed, a collective decision-making model has been successfully implemented by other digital platform regulators, such as the Australian Communications and Media Authority (ACMA) and the Australian Competition and Consumer Commission.

The Government will consider options for transitioning eSafety to a multi member governance model to support robust decision making for online safety regulation (recommendations 58, 59, 61, 62).

The Government is committed to Budget sustainability, including cost recovery mechanisms to fund government services where appropriate. The Government will consider the potential benefits and impacts of further extending any cost recovery to the regulation of the Act in accordance with the Australian Government Cost Recovery Policy, and any learnings from adjacent efforts in regulating and recovering costs from digital platforms in other portfolios (recommendation 63, 64).

Review Recommendation	Government Response
58: To support collective decision making, the regulator should move to a Commission model of governance and be known as the 'Online Safety Commission'.	Support in principle
59: That the Commission should be comprised of a Chair, Deputy Chair and a Commissioner, with flexibility for the	Support in principle

Commission to grow up to nine members as the functions and powers of the regulator increase.	
60: That in moving to a Commission, the Act should require Commission members to have an appropriate mix of skills to support informed and robust decision-making.	Support in principle
61: That a newly formed Commission has strong internal governance processes, is transparent in how it does its work, and ensures that it reports meaningfully on its performance.	Support in principle
62: That following consideration of the regulator's functions and responsibilities under a new regulatory framework, the regulator should transition to a standalone, independent regulator to support its growing functions and responsibilities, and to future-proof the regulator.	Note
63: That the regulator should be appropriately resourced to implement the right regulatory infrastructure and carry out its functions. This includes having an ongoing dedicated and appropriately resourced legal team, appropriate corporate management and the information technology it needs to do its job well. Consideration should be given to how other regulators operate to determine what may be appropriate in the regulator's context.	Support
64: A cost recovery mechanism should be developed to fund the cost of regulating industry, with details to be settled by government in consultation with industry.	Note

The Road Ahead

The Government recognises the need to ensure reforms to the Act meet their intended objectives and for this to be assessed through an independent process. Provisions will be included for a further statutory review of the Act within three years of commencement of the new legislation (recommendation 66).

Key reforms arising from the review, such as the duty of care and associated reforms, will be prioritised for implementation. The Government will also prioritise consideration of appropriate governance arrangements and resourcing for the regulator (recommendation 65).

The Government notes the recommendation for future consideration of a centralised online harms regulator noting the formation in 2022 of the Digital Platform Regulators Forum (DP-REG) to address the risks and harms faced by Australians in the online environment. DP-REG consists of the Australian Competition and Consumer Commission, the Australian Communications and Media Authority, the eSafety Commissioner and the Office of the Australian Information Commissioner (recommendation 67).

The Forum is an information-sharing and collaboration initiative between Australia's independent regulators with a shared goal of ensuring Australia's digital economy is safe, trusted, fair, innovative and competitive.

Review Recommendation	**Government Response**
65: That if required, the Government should prioritise implementation of the key reforms arising from this review that will provide the most substantial and immediate online safety protections for Australians, including in particular the new duty of care and associated reforms. This should coincide with the regulator moving to a Commission model of governance and appropriate resourcing to support the implementation of priority reforms.	Note
66: That the updated Act be subject to independent review within three years of the commencement of the key reforms to the Act, or by 2029, whichever is earliest.	Support
67: That the Government consider how its existing administrative arrangements relating to online harms are operating and whether there is a case for having a central online harms regulator. Given the level of change that needs to happen now to better protect Australians, this consideration may be best left to around the time of the next review.	Note