AER Electricity Distribution Ring-Fencing Guideline - Compliance reporting best practice manual

Version 1

June 2018

AUSTRALIAN ENERGY REGULATOR

Inquiries about this publication should be addressed to:

Australian Energy Regulator
GPO Box 520
Melbourne Vic 3001

Tel: 1300 585165

Email: ringfencing@aer.gov.au
AER Reference: 62887/D18-12543

Amendment Record

Version	Date	Pages
1	8 June	20

Contents

1 Introduction

1.1 Purpose of this document

The purpose of this compliance reporting manual is to inform distribution network service providers (**DNSP**s) of the **AER**'s view regarding their compliance reporting obligations under the **Ring-fencing Guideline – Electricity Distribution** (the **Guideline**).[1] It should be read in conjunction with the **Guideline** and its accompanying explanatory statements.[2] This document covers the entire suite of compliance obligations set out in the Guideline, including:

- breach reporting
- maintenance of registers
- annual compliance reporting
- annual independent assessments of compliance
- complaints and investigations

The manual provides detailed guidance on the **AER**'s interpretation of the compliance reporting requirements in the **Guideline**. This manual does not impose additional requirements on DNSPs. The requirements of the **Guideline** are binding under clause 6.17.1 of the **National Electricity Rules**.

This manual is consistent with the **AER**'s *Compliance and Enforcement Approach*.[3]

This manual may be updated from time to time by the **AER**. All changes will be designed to increase the clarity surrounding our expectations as to how **DNSP**s should satisfy compliance reporting requirements under the **Guideline**.

1.2 The Ring-Fencing Guideline

The **Ring-fencing Guideline – Electricity Distribution** was made under clause 6.17.2 of the **National Electricity Rules**. It was first published in November 2016 and amended in October 2017.

The objective of the **Guideline** under clause 1.1.1 is to:

- promote the **National Electricity Objective** by providing for the accounting and functional separation of the provision of **direct control services** by **DNSP**s from the provision of other services by them, or by their **affiliated entities**.

---

[1] AER, Ring-fencing Guideline – Electricity Distribution – Version 2, October 2017, https://www.aer.gov.au/networks-pipelines/guidelines-schemes-models-reviews/electricity-ring-fencing-guideline-october-2017

[2] AER, Ring-fencing Guideline – Electricity Distribution – Version 2 – Explanatory Statement, October 2017, https://www.aer.gov.au/networks-pipelines/guidelines-schemes-models-reviews/electricity-ring-fencing-guideline-october-2017; AER, Electricity Distribution Ring-fencing Guideline – Explanatory Statement, December 2016, https://www.aer.gov.au/system/files/AER%20Ring-fencing%20Guideline%20-%20Explanatory%20statement%20-%2030%20November%202016.pdf

[3] AER, AER Compliance and Enforcement – Statement of Approach, April 2014, https://www.aer.gov.au/publications/corporate-documents/aer-compliance-and-enforcement-statement-of-approach

- promote competition in the provision of electricity services.

It aims to accomplish this objective by imposing obligations on **DNSP**s, targeted at, among other things:

- cross-subsidisation, with provisions that aim to prevent a **DNSP** from providing **other services** that could be cross-subsidised by its **distribution services**; and
- discrimination, with provisions that aim to:
    - prevent a **DNSP** conferring a competitive advantage on its **related electricity service providers** that provide **contestable electricity services**; and
    - ensure a **DNSP** keeps information it acquires or generates confidential, and handles that information appropriately.

1.3 Terminology

For the purposes of this manual, all bold terms have the meaning defined in the clause 1.4 of the **Guideline** or the **National Electricity Rules**.

2 Compliance breaches

Clause 6.3 of the **Guideline** requires a **DNSP** to notify the **AER** in writing within five business days of becoming aware of a material breach of its obligations under the **Guideline**.

The **AER** aims to foster and promote a culture of compliance.[4] Under the **National Electricity Rules**, the **AER** does not have the power to impose civil penalties with respect to ring-fencing. Our enforcement approach is focussed on creating a long term, sustainable environment of compliance that will give confidence to the market. **DNSPs** should consider informally engaging early with the **AER** when they identify breaches, to notify us of the breach and allow the **AER** to respond effectively.

2.1 Materiality

The **AER** interprets 'material' in this context to mean 'something that is more than trivial'. Note that 'material' in the **Guideline** has a different meaning to other contexts where the **AER** might use this term, where materiality is defined by reference to a quantitative threshold.[5] The **AER** may choose to supplement the definition of a material breach over time.

When assessing whether or not a breach is material, the **AER** recommends **DNSPs** consider the entire context in which the breach occurs. Factors for consideration could include, but are not limited to:

- whether the breach has resulted in cross subsidy of **other distribution services** or **other services**,
- whether the breach has compromised the functional separation of **direct control services** from **other distribution services** or **other services**,
- whether the breach is likely to cause a competitive advantage to a **related electricity service provider** with respect to performing **contestable electricity services**,
- whether the breach involved the disclosure of confidential information,
- whether the breach is likely to be ongoing,
- whether this is a recurrence of similar past breaches,
- the seniority of staff within the **DNSP** or **affiliated entity** that have committed the breach,
- the degree of effort required to rectify the breach, or
- whether the breach forms part of a course of conduct that may impact the objective of the **Guideline**.

[4] AER, AER Compliance and Enforcement – Statement of Approach, April 2014, https://www.aer.gov.au/publications/corporate-documents/aer-compliance-and-enforcement-statement-of-approach, p. 5

[5] For clarity, the NER Chapter 10 definition 'materially' that applies to the use of this word in clause 6.6.1 and clause 6A.7.3 does not apply to this context which deals with material breaches of obligations in the **Guideline**.

If, once a breach has been assessed by the **DNSP**, there is more than a passing or momentary concern in any category, the breach is likely to be more than trivial and therefore material. For clarity, the mere fact that the **DNSP** acts on internal processes to assess a breach does not make it more than trivial. For each breach identified, the **DNSP** will likely need to undertake some analysis to determine the materiality of that breach.

2.2 Timeframes for reporting of material breaches

The **Guideline** states that **DNSP**s must report material breaches to us in writing within five business days of becoming aware that the breach has occurred. We interpret 'five business days' to start the day after the breach is discovered.[6] For example, if a breach is discovered on Tuesday 5 June 2018. 'Day 1' of the five business days would be Wednesday 6 June 2018. The end of the five day period would be on Tuesday 12 June 2018.

2.3 Breach reporting templates

The **AER** has provided two templates for reporting material breaches under clause 6.3 of the **Guideline**:

- A cover letter template for reporting of material breaches (word document)
- A breach reporting template for reporting of material breaches (spreadsheet)

The reporting template guides the form and content of the initial report. It requires the reporting of specific information, including: (1) a description of the breach (obligation breached, dates over which breach occurred and the nature of the breach); (2) how the breach was identified; (3) the impact of the breach on achieving the **Guideline** objectives in clause 1.1.1 of the **Guideline**; (4) remediation measures that the **DNSP** has taken or plans to take, and; (5) any past breaches of the same **Guideline** obligation. The final column, 'other', allows **DNSP**s to add any additional information at their own discretion. These templates are available on the AER website.

DNSPs should email breach reports to ringfencing@aer.gov.au and clearly identify that they are reporting a breach.

While these templates are for guidance, when it comes to material breaches we strongly suggest that **DNSPs** make use of them in order to allow the AER to assess initial data in a timely manner. We have made the breach reporting template purposefully brief to enable **DNSP**s to report promptly on breaches. In addition to the letter and spreadsheet breach report templates, a DNSP may provide any further attachments it considers pertinent to the matter. This can be done at the **DNSP**'s discretion and must not hold up timely reporting of breaches to the **AER**.

To that end, in order to use the suggested templates effectively and ensure that the Guideline requirements are met;

- The template cover letter should be signed by an **officer** responsible for the most relevant division of the business.

[6] Clause 28 to Schedule 2 to the National Electricity Law

- **DNSP**s should report one breach per row of the breach reporting template spreadsheet. Should a **DNSP** wish to report multiple breaches at the same time they can use one breach report file to report multiple breaches, with each breach being a new row in the template.

3 Public registers and protocols

The Guideline requires **DNSP**s to maintain three publicly available registers:

- Office and staff register[7]
- **Information register**[8]
- Waiver register.[9]

In addition, the **DNSP** must establish a publicly available information sharing protocol.[10]

DNSPs should carefully consider the form, content and accessibility of these registers. A register or protocol that is generic or high level may not contain enough detail to fulfil the requirements of the **Guideline**. Similarly, if members of the public struggle to locate these registers and protocols on the website, they may not have the effect of preventing discrimination intended by the **Guideline**.

Registers should be updated continuously (for example, when new information needs to be added to the information register) and reviewed regularly to ensure that the information remains current.

Information on the **information and staff sharing registers** should be retained for a sufficient period of time to allow that information to be effectively accessed by third parties, including **related electricity service providers** and other legal entities who provide **contestable electricity services** but who are not **affiliated entities**. **DNSP**s should also ensure that the terms of their information sharing protocol do not unnecessarily restrict the ability of any **legal entity** to access information on the register, or be added to the **information register**.

[7] Required by clause 4.2.4 of the **Guideline**

[8] Required by clause 4.3.5 of the **Guideline**

[9] Required by clause 5.7 of the **Guideline**

[10] Required by clause 4.3.4 of the **Guideline**

4 Annual Compliance Report

Clause 6.1 of the **Guideline** requires that a **DNSP** establish and maintain appropriate internal procedures to ensure it complies with its obligations under the **Guideline**.

Clause 6.2.1 (a) of the **Guideline** mandates that a **DNSP** prepare an annual report on ring-fencing compliance and submit it to the **AER**. Clause 6.2.1(b) of the **Guideline** lays out four categories of information that must be included in all annual compliance reports. The following sections lay out the **AER**'s view on compliance reporting for each of these categories.

We expect that annual compliance reports should be accompanied by a cover letter signed by the CEO or acting-CEO of the **DNSP** attesting that the contents of the report are accurate to the best of their knowledge.

4.1 Measures to ensure compliance

Sub-clause 6.2.1(b)i states that a **DNSP** must identify and describe "the measures the **DNSP** has taken to ensure compliance with its obligations under this **Guideline**". In its annual compliance report, **DNSP**s should explain how the compliance measures put in place address every obligation in the **Guideline**. **DNSP**s should also demonstrate in their annual report that there are a range of controls in place to address risk of non-compliance for each obligation, as relevant. For example, in assessing the appropriateness of a **DNSP**'s compliance measures, the **AER** will consider whether each obligation is addressed by:

- 'Preventative' controls or measures, which are designed to prevent breaches of a particular obligation in the **Guideline** from occurring;
- 'Detective' controls or measures, which are designed to ensure that breaches that have already occurred can be detected or identified internally in a timely way;
- 'Corrective' controls or measures, which ensure that timely and appropriate corrective or remedial action can be taken to address a breach once is detected. Having strong corrective controls in place may make breaches less likely to recur.

DNSPs may choose to structure their annual reporting by identifying ring-fencing obligations and identifying the compliance controls that apply to each obligation. Or **DNSP**s may choose to structure their annual report by identifying the main compliance controls they have put in place. If the latter approach is adopted, it is important that **DNSP**s clearly map the range of compliance controls they have in place back to each ring-fencing obligation, so that it is clear how compliance with each obligation is being met.

4.1.1 Meaningful compliance reporting

In general, we encourage DNSPs to adhere to the following principles when writing their annual compliance reports:

- Report on specific measures, areas of the business, or challenges, rather than describing compliance measures in general, vague, or abstracted terms.

- Hone in reporting on areas of the business that carry greater risk of breaches of the **Guideline** or which have experienced breaches over the course of the **regulatory year** and focus reporting on those areas.
- Avoid jargon and technical language where possible and keep compliance reporting clear and as 'plain English' as possible.

Reporting that only describes compliance measures at a very high level can make it difficult for the reader to understand what specific measures have actually been undertaken. It is important that broad descriptions of overarching compliance measures are supported by more specific and tangible analysis of how those overarching compliance principles are being put into practice. In particular, **DNSP**s should consider providing greater detail on how ring-fencing safeguards are being put into practice in higher risk areas of the business, and whether those safeguards have been demonstrated to be adequate.

4.2 Breaches

Under clause 6.2.1(b)ii any breaches of the **Guideline** by the **DNSP** must be reported in the annual compliance report. This means that any material breaches already reported to the **AER**, and any breaches not already reported to the **AER**, must be reported upon within the annual compliance report. Under clause 6.3 of the **Guideline**, a **DNSP** must notify the AER in writing within five business days of becoming aware of a material breach of the **Guideline**.

DNSPs must also report on any breaches that relate to the **DNSP** under clause 6.2.1(b)ii of the **Guideline**. Therefore, any breaches in respect of service providers (pursuant to 4.4.1) and other breaches that relate to a **DNSP** must be recorded in the annual compliance report.

4.3 Other services

Clause 3.1 of the **Guideline** sets out the specific circumstances under which **DNSP**s can provide **other services** without breaching the **Guideline**. In accordance with 6.2.1(b)iii these services must be reported in the annual compliance report.

In order to adequately demonstrate that any **other services** are provided in accordance with the **Guideline**, **DNSPs** should describe each service clearly and in sufficient detail so that it is clear what the nature of the service it that is being delivered. **DNSP**s should also describe any measures or controls that have been put in place in relation to the delivery of other services to comply with the **Guideline**.

4.4 Transactions with affiliated entities

Clause 6.2.1 (b)iv of the **Guideline** requires a **DNSP** to report on the purpose of all transactions between the **DNSP** and its **affiliated entities**. Where a set of individual transactions share a common purpose, the **DNSP**s may group those together with the number of transactions and the total dollar value to be recorded in their respective columns. Transactions share a common purpose if they form part of the same course of transactions, are for the same or similar items, or there are other factors that indicate that the transactions are substantially similar.

DNSPs should also identify the affiliate entity involved in the transactions. We expect that reporting on transactions with **affiliated entities** should be underpinned by accounts that

conform to relevant standards and requirements in the Corporations Act. The **AER** may require that the **DNSP** submit relevant accounts related to transactions with **affiliated entities** in accordance with clause 6.4, clause 3.2.1(a)i, and clause 3.2.1(a)ii of the **Guideline**.

To assist the **AER** in interpreting this data and maintaining a working knowledge of relevant compliance arrangements, **DNSP**s should consider providing the **AER** with a complete list of all of the **DNSP**'s **affiliated entities** as part of their annual report.

5 Independent compliance assessment

Clause 6.2.1(c) of the **Guideline** requires that a **DNSP**'s annual compliance report be accompanied by an assessment of compliance by a suitably qualified independent authority. **DNSP**s will bear the cost of this assessment.

5.1 What is a 'suitably qualified independent authority'?

The **AER** will need to be satisfied that any party selected by the **DNSP** to provide an assessment of compliance is both independent and suitably qualified. We discuss each concept below.

5.1.1 Independence

Independence means that the person conducting the assessment should not be a director, **officer** or employee of the **DNSP** or an **affiliated entity** (including parent or associate companies whether in Australia or overseas), and there should be no perceived linkages or conflicts of interest that would prevent the assessor from entering into an assurance agreement.

DNSPs should engage an external third-party compliance assessor to conduct the assessment.

DNSPs may engage third-party assessors that have previously been contracted to do work for the **DNSP**. For example, a third-party that provides Regulatory Information Notice auditing or other regulatory services for the **DNSP** may also be engaged to provide independent assessment of ring-fencing compliance.

DNSPs and assessors should apply established codes of conduct and standards in order to demonstrate professional independence.

We expect that **DNSP**s should rotate their independent assessors from time to time to ensure that the assessor's independence is not compromised by performing many successive assessments of the **DNSP**'s ring-fencing compliance. **DNSP**s should rotate independent assessors at least every five years.

5.1.2 Suitably qualified

A suitably qualified assessor should have a track record of contracted compliance assessment and audit engagements across a range of different past clients. An assessor that had only undertaken a limited number of compliance engagements, or who had only undertaken compliance engagements for a small number of clients in the past may not be judged by the **AER** to be suitably qualified. The **AER** considers that an assessor who meets the requirements in ASAE 3000, ASAE 3100, ASQC 1 or another similar standard will be suitably qualified.

5.1.3 Demonstrating that an assessor is suitably qualified and independent

In order to satisfy the requirements under clause 6.2.1(c) of the **Guideline**, the assessor's report should include a statement demonstrating that the assessor is both a "suitably qualified" and an "independent" authority. We expect that this could be achieved by:

- A statement regarding any relevant professional standards and codes of conduct that were applied to the assessment engagement, and why those were the most appropriate standards and codes of conduct to satisfy the **Guideline** requirements.
- Providing a conflict of interest statement signed by the independent assessor, which would describe any real or perceived conflicts of interest and explain how they have been managed through the course of the assessment engagement.

5.2 Assurance Level

The independent assessor should be engaged to provide *reasonable assurance* that the DNSP has complied with the **Guideline**.[11] This means that the assessor should provide assurance that:

- Compliance measures or controls reported by the **DNSP** in its annual report are reflected in day-to-day business practices and are appropriate with respect to the **Guideline** obligations.
- All breaches that the organisation is aware of are accurately reflected in the compliance report, and that the description clearly and accurately reflects the nature and cause of each breach.
- All **other services** provided by the **DNSP** are accurately recorded in the compliance report.
- Transactions reported under 6.2.1(b)iv are an accurate reflection of all agreements, arrangements or other dealings (including in relation to the supply of goods or services) between the **DNSP** and its **affiliated entities**, and the purpose of those transactions is accurately reflected in the report.

The requirements laid out in the ASAE 3100 standard (or another similar standard deemed appropriate in the circumstances by the independent assessor) could serve as a basis for this analysis.

In order to establish the assurance level of the independent assessment, we would also expect to see the following included in the annual report and independent assessor's report:

- Details of the assessment methodology and how relevant standards were used to design that methodology and implement the assessment. This could include a description of the type of sampling and auditing procedures used to assess **DNSP** compliance against ring-fencing obligations, and how the assessment methodology aligns with relevant ISO or ASAE standards chosen to guide the assessment. This statement should be sufficient to enable the **AER** to conclude that the assessment methodology was robust enough to satisfy the requirement for reasonable assurance.

[11] "Reasonable assurance" is defined in Australian Standards Board, ASAE3000: Assurance Engagements Other than Audits or Reviews of Historical Financial Information.

- A statement from the assessor detailing any limitations of the assessment, and areas of the assessment where information was inconsistent, incomplete, or incorrect, and the degree to which this has negatively impacted the assurance level.

The **AER** considers that the assurance level required to demonstrate compliance in relation to ring-fencing is higher than in other circumstances, such as regulatory information notices. This is due to the highly qualitative nature of ring-fencing compliance. The **AER** may consider requesting a lower level of assurance in future years, or limiting the scope of the assessment, once **DNSP**s establish a solid base of demonstrated compliance.

The assessors report should clearly identify the nature of any issues, concerns, and recommendations for improvement that were raised in the course of the independent assessment that may or may not have been subsequently addressed by the **DNSP**.

5.3 Pre- and post-assessment meetings

The **AER** may request meetings with the **DNSP**'s chosen independent assessor prior to the commencement of the assessment and after the annual report and independent assessment has been submitted. A pre-assessment meeting between the **AER** and the independent assessor will provide the assessor with an opportunity to understand the **AER**'s overall expectations for independent assessments. A post-assessment meeting will provide the **AER** with an opportunity to question and clarify aspects of the **DNSP**'s annual report and independent assessment report.

The **AER** will inform the **DNSP** in writing of pre and post-assessment meetings and will coordinate with the **DNSP** and the independent assessor to organise these meetings.

5.4 Outcomes of the assessment

Broadly speaking, the **AER** expects that an independent assessment of compliance should clearly address core ring-fencing compliance issues, including but not limited to:

- Were any previously unknown or unreported compliance breaches discovered as a result of the assessment?
- What areas of ring-fencing compliance were identified as being weak or at risk of future breaches and why?
- What areas of ring-fencing compliance were identified as being strong or at low risk of future breaches and why?
- What recommendations does the assessor have to improve the **DNSP**'s ring-fencing compliance framework?

The **DNSP** may also provide information to the **AER** regarding how the **DNSP** intends to respond to any recommendations for improvement raised by the independent assessor.

5.5 Types of assessment

DNSP independent assessments should provide reasonable assurance covering all obligations within the **Guideline**. However, the **AER** may consider targeted compliance assessments in the future. This could allow the **AER** to target specific areas of compliance for independent assessment in the future or opt for an independent assessment on the basis

of limited assurance. Changes to the scope of future reviews would be contingent upon **DNSP**s establishing a solid base of demonstrated compliance. Prior to adjusting the mode of assessment the **AER** would consult with **DNSP**s.

6 AER compliance investigations and reporting

6.1 Our response to reporting of material breaches by DNSPs

DNSPs should report material breaches within 5 business days by sending their breach report to ringfencing@aer.gov.au as per section 2.2 of this manual. The **AER** will assign an individual breach number to each reported breach, which **DNSP**s should retain for their records. **DNSP**s should quote this breach number if reporting on future related breaches.

In assessing a breach reported by a **DNSP**, we may ask the **DNSP** to provide additional information under clause 6.4 of the **Guideline**. This will be an opportunity for the **DNSP** to provide greater detail and analysis surrounding the breach that is targeted to the needs of our investigation. As noted in our Explanatory Statement, we expect that **DNSP**s will have a strong incentive to provide such follow-up details.[12] Where circumstances warrant, we may also require that the **DNSP** provide regular updates on the status of the breach until we are satisfied that the breach has been rectified.

6.1.1 Publication of breaches

If a breach is considered material, but does not pose a serious risk to achieving the aims of the **Guideline**, the breach may be reported in the **AER**'s Quarterly Compliance Report.

Where the **AER** considers that a breach is more serious, and that the market would benefit from a timelier reporting of the breach, we may issue a communications notice or media release, or publish information about the breach in another form, on the **AER** website.

In determining the seriousness of the breach, the **AER** will apply the considerations laid out in section 2.1 of this manual with regard to materiality, as well as other factors such as:

- Previous breaches of the obligation, and
- Whether there is a need for immediate reporting in order to inform market participants that may be affected by the breach.

6.2 Our response to annual compliance reports

The **AER** may report on ring-fencing compliance from time to time, drawing upon **DNSP** annual compliance reporting, breach reporting, and our own investigations. The purpose of this reporting will be twofold:

1. Increase the transparency of the ring-fencing regime in order to maintain confidence in the competitiveness of markets for contestable electricity services. This will support achieving the **Guideline**'s objective of promoting competition in the provision of electricity services.
2. Aid **DNSP**s in strengthening measures that can prevent breaches of the **Guideline** from taking place. Our reporting will focus on creating a culture of compliance by

[12] AER, Electricity distribution Ring-fencing Guideline: Explanatory statement, November 2016, p.68

DNSPs and their affiliate entities, in line with our *Compliance and Enforcement Statement of Approach*.

A **DNSP**'s compliance measures may be found to be weak as a result of the ring-fencing compliance annual report and accompanying independent assessment. This could be evidenced by systemic breaches that have already taken place, or perceived risk that breaches may take place in the future as a result of poor compliance measures. If this occurs the **AER** will take steps, including engaging with the business and affected parties to determine what compliance measures are required.

6.2.1 Publication of DNSP annual ring-fencing compliance and independent assessment reports

The **AER** will publish **DNSP** ring-fencing compliance reports and the accompanying independent assessment on the **AER** website.

DNSPs may also elect to provide a confidential version of the annual compliance report and/or the independent assessor's report to the **AER**. Should **DNSP**s wish to report information in confidence, they can do so in accordance with the AER's Confidentiality Guideline.

This process requires that **DNSP**s:

1) Engage with the **AER** to discuss their confidentiality claim prior to lodgement of the document. The **AER** will work with **DNSP**s to reach a shared understanding of the confidentiality issues involved.

2) Submit a confidentiality template, as laid out in the Confidentiality Guideline, together with public and confidential version of the annual compliance and independent assessment reports.

3) Engage with our stakeholder information process. The **AER** is unlikely to disclose information publicly where we consider that stakeholders have been given enough information to satisfy the objectives of Ring-fencing **Guideline**. If the **AER** considers that claimed confidential information is central to achieving these objectives we will engage with the **DNSP** to determine an approach to this information. This might involve measures such as narrowing the confidentiality claim, or adjusting the information to protect sensitive elements.

6.3 Our approach to handling ring-fencing complaints

Clause 6.4 of the **Guideline** allows the **AER** to require a **DNSP**s to provide a written response to a complaint or concern the **AER** raises with the **DNSP** about its compliance with the **Guideline**. Clause 6.1 of the **Guideline** allows the **AER** to require the **DNSP** to demonstrate the adequacy of internal compliance procedures upon reasonable notice. We will seek information from **DNSP**s in response to complaints or concerns where we consider that there are reasonable grounds for investigating these matters further.