EXTERNAL REVIEW OF THE AUSTRALIAN ELECTORAL COMMISSION TRANSPARENCY REGISTER DATA BREACH

Contents

Summary 2
Terms of Reference 4
List of abbreviations, acronyms, key definitions 5
List of Recommendations 6
List of Findings 7
Introduction 9
Term of Reference #1: How did this data breach occur? 11
Term of Reference #2: What is the extent of the Data Breach? 20
Term of Reference #3: Has the AEC remediated the issue to the best extent possible? 26
Term of Reference #4: What lessons does the AEC need to implement to minimise the risk of similar breaches in the future? 31
Appendices 37

Classification: OFFICIAL

Summary

On 15 May 2024 the AEC discovered an inadvertent **data breach** on its Transparency Register (the Register), which led to the current silent elector addresses of 71 election candidates, including some current parliamentarians, to be published on the Register for up to nearly five years. AEC records show that the addresses of 17 of those 71 were publicly viewed. The data breach potentially put these individuals at serious risk of harm. The data breach was the result of a process error not a cyber security breach.

The AEC made a working-level decision when the Register was being developed in 2019 to include addresses in entity headers or 'banners'. The inclusion of an address in the banner was unnecessary but not unreasonable.

A second working-level decision was made to draw these addresses from the postal address field of election candidate nomination forms. Using addresses from candidate nomination forms when they were not provided for that purpose was the wrong thing to do. It was the primary cause of the data breach.

The AEC's Executive Leadership Team was unaware of that decision, which reflected inadequate project governance and escalation of risk.

It would have been very difficult to foresee that addresses in banners on the Register could lead to silent addresses being published. The AEC did not identify that risk and did not discover the issue until a parliamentarian saw their silent address on the Register and questioned it.

In the course of investigating the source of the data breach the AEC recognised a separate **data release** issue. In accordance with its legislation the AEC publishes completed election returns on the Register in their original form. In an instance where an entity erroneously provided a silent elector address, or legitimately provided an address that became silent later, then those addresses were also accessible on the Register. Addresses from returns were not visible in entity banners and could only be accessed by searches on the Register or by viewing a specific PDF.

The AEC is not currently in a position to advise the extent of the data release. It will have had the potential to affect only a very small minority of those whose addresses appear on the Register and will not have affected anyone who had not put in a disclosure return or been named in one.

The AEC took the Register offline on 15 May 2024, temporarily remediating both the data breach and data release. This was an appropriate course of action noting the important role suppression of silent elector addresses plays in protecting the personal safety of those electors who may be at risk. The Review notes that as of 25 July 2024 the AEC had reinstated the Register on its website without including addresses in entity banners or PDFs of original returns.

The AEC prioritised communication with the Australian Federal Police (AFP) about the data breach. The AFP advised the Review that the AEC's communication lowered the operational risk this presented. The AFP is not aware of any personal safety incidents as a result of the data breach to this point. The AEC has also briefed the AFP on the data release issue.

Because some silent addresses were publicly viewed before the remediation, the risks posed by the data breach are ongoing. The AEC's regular and close communication with AFP will be important to help lower the potential risk to personal safety as much as possible.

The AEC reported the data breach to the Office of the Australian Information Commissioner (OAIC) under the Notifiable Data Breaches Scheme. It also notified those impacted by the breach. The OAIC has confirmed with the Review that the AEC has met its obligations under the scheme.

The AEC assesses that the data release does not constitute a notifiable breach. The Review agrees with this position.

The Review contains eight recommendations and 19 findings. Most important of the recommendations is that the AEC remove or redact silent elector addresses prior to putting the Register back online.

Noting the AEC is required by legislation to publish returns on the Register, there is also a recommendation to amend the *Commonwealth Electoral Act 1918* (the Electoral Act) to require publication of returns information rather than the returns themselves and to give AEC the power to redact, remove or amend personal information on the Register.

The AEC's management of the incident since 15 May 2024 has demonstrated the strength of its crisis response capability. The commitment the AEC has shown to exposing and fixing the problems with the Register also speaks well to its culture. But work clearly needed to be done at the AEC in the areas of project governance and risk management. The 2019 project governance for the development of the Register was insufficient. And it took almost five years for anyone to discover the breach, which is also of concern.

The AEC has made significant improvements to its project governance and risk management since 2019. Nevertheless, there are recommendations and findings that the AEC should consider carefully to avoid a repeat of this regrettable breach, and to minimise the ongoing risk the data breach and data release present.

Terms of Reference

On 17 May 2024, the Electoral Commissioner, Tom Rogers, announced that there would be an external review of the AEC Transparency Register.

On 4 June 2024, external reviewer Tony Sheehan commenced the external review with the following Terms of Reference:

The reviewer should work to determine responses to the following questions:

1. How did this data breach occur?
2. What is the extent of the data breach?
3. Has the AEC remediated the issue to the best extent possible?
4. What lessons does the AEC need to implement to minimise the risk of similar breaches in the future?

List of abbreviations, acronyms, key definitions

AC	AEC Assistant Commissioner
AEC	Australian Electoral Commission
AFP	Australian Federal Police
Agile	A project management approach that involves breaking the project into phases, emphasizing continuous collaboration and improvement and following a cycle of planning, executing, and evaluating.
ANL	Australian National Library
APSC	Australian Public Service Commission
Data Breach	The erroneous exposure of silent elector addresses in some candidate entity banners on the Transparency Register.
Data Release	The publication of some silent elector addresses as an unintended consequence of AEC meeting its legislative obligations to publish returns on the Transparency Register.
DTA	Digital Transformation Agency
ELMS	Electoral Management System
ELT	AEC Executive Leadership Team
FAC	AEC First Assistant Commissioner
FAD	Funding and Disclosure
ICMF	AEC Incident and Crisis Management Framework
ICT	Information and Communications Technology
IMT	AEC Incident Management Team
Indigo	A multi-year, business-led program to transform and modernise the AEC's core ICT infrastructure and capability
NIM	AEC National Incident Manager
OAIC	Office of the Australian Information Commissioner
PDF	Portable Document Format – a file format for capturing and sending electronic documents in the intended format.
PIA	Privacy Impact Assessment
PRINCE2	A process-based methodology for project management
SCC	Security Coordination Committee
SES BAND 2	Senior Executive Service level Australian Public Servant
SSP	AEC Self-Service Platform (the 2019 project of which the Register was a part)
The Electoral Act	*The Commonwealth Electoral Act 1918*
TIC	AEC Transformation and Investment Committee
Trove	An Australian National Library digital platform that provides access to over 6 billion information items from around 900 Australian institutions.

List of Recommendations

- **Recommendation 1**
  That the AEC audit those of its systems which do not automatically supress silent elector addresses, so it is positioned to identify, and where necessary supress, any silent elector addresses present on those systems.

- **Recommendation 2**
  That AEC review its management of website and Transparency Register maintenance and curation, to ensure these roles and responsibilities are clear across the organisation.

- **Recommendation 3**
  That the AEC's Crisis and Incident Management doctrine include explicit guidance on consultation with other agencies.

- **Recommendation 4**
  That the AEC remove addresses from Transparency Register entity banners.

- **Recommendation 5**
  That the AEC recommends to government and the Department of Finance an amendment to the *Commonwealth Electoral Act 1918,* which requires publication of returns information rather than publication of returns. The amendment should also give AEC the power to redact, remove or amend information on the Transparency Register including past returns and information provided prior to the amendment coming into effect.

- **Recommendation 6**
  That the AEC redact or remove silent elector addresses prior to putting the Transparency Register back online.

- **Recommendation 7**
  That the Electoral Commissioner review the 'approved forms' for returns on the Transparency Register to ensure the forms seek only the information required by the *Commonwealth Electoral Act 1918*.

- **Recommendation 8**
  That the AEC conduct a desktop exercise of its current ICT project governance framework using a contemporary scenario along the lines of the data breach to satisfy itself that it has mitigated the risk of a similar incident in the future to the extent possible.

List of Findings

- **Finding 1**
  The inclusion of an entity address field in the Transparency Register from 2019 was unnecessary and regrettable, but in the context of a transparency measure, not unreasonable.

- **Finding 2**
  The AEC was wrong to publish postal addresses from candidate nomination forms in the Transparency Register entity banners as those addresses were not collected for that purpose. It was the primary reason for the data breach.

- **Finding 3**
  Senior officers in the AEC were unaware of the undocumented working-level technical decision to include postal address data from candidate nomination forms in the entity banners on the Transparency Register. The governance around the erroneous decision was not sufficient.

- **Finding 4**
  The lack of any formal documented decision to include an address in entity banners on the Transparency Register, and the junior level within AEC at which the inclusion of the address field was considered, contributed to the data breach remaining undetected for as long as it did.

- **Finding 5**
  In the course of the data breach investigation, AEC recognised a separate data release risk. Silent elector addresses had been inadvertently provided to the AEC, or had become silent after being provided, in returns published on the Transparency Register in accordance with the *Commonwealth Electoral Act 1918*.

- **Finding 6**
  The AEC temporarily remediated the separate data release risk in Finding 5 at the same time that it remediated the data breach, by taking the Transparency Register offline. How many silent addresses were in published returns and whether they were accessed is not known at the time of the Review.

- **Finding 7**
  That 2680 candidates were technically affected by the data breach. For the vast majority the breach had no practical impact. For 71 individuals the breach caused a potentially serious risk to personal safety. The addresses of only 17 of the 71 were actually viewed as a result of the data breach. This figure of 17 does not account for any current silent addresses provided in returns on the Transparency Register (“the data release”) that may have been publicly accessed.

- **Finding 8**
  Based on consultation with the Australian Federal Police, the Review finds that the incident response, mitigation and communication steps taken by the AEC upon discovery of the data breach, lowered the risk to personal safety of the data breach.

- **Finding 9**
  Based on advice from the Australian Federal Police the Review finds that there has not been any personal safety impact from the data breach at the time of writing. This is necessarily a point in time finding only.

- **Finding 10**
  Based on consultation with the Office of the Privacy Commissioner, the Review finds that the AEC has met its privacy responsibilities to the Australian Information Commissioner and the public in the way it has communicated the notifiable data breach and provided information about it.

- **Finding 11**
  It is unavoidable that the data breach will have had some impact on the AEC's strong reputation for securely managing information. Its ongoing actions since the data breach will help minimise that impact.

- **Finding 12**
  The AEC Incident and Crisis Management Framework, which governed the incident response, is well constructed, connected to broader Commonwealth government crisis arrangements and effectively implemented. This contributed to the swift remediation of the data breach and risks it presented.

- **Finding 13**
  The Electoral Commissioner took the only viable course of action to achieve short-term technical remediation of the publishing of silent elector addresses by taking the Transparency Register offline.

- **Finding 14**
  The AEC should continue its work in communicating personally with those who have been affected by the data breach or data release and are assessed to be at high risk.

- **Finding 15**
  The AEC has remediated both the data breach and data release issue to the best extent possible to this point. Remediation, risk mitigation and communications work are ongoing and, in some areas, subject to acceptance of the Review's recommendations.

- **Finding 16**
  That a brief module on risk management that recognises the expectations at different work levels, be incorporated into the AEC Mandatory Learning Program to provide further assurance to AEC.

- **Finding 17**
  The AEC has implemented necessary changes to governance and project management of ICT projects in the AEC to minimise the risk of a future data breach similar to that which occurred with the Transparency Register.

- **Finding 18**
  The AEC should review its Risk Register horizon scanning approach to ensure it is rigorous, regular and informed by changes in technology, and the internal and external security and privacy context.

- **Finding 19**
  The AEC should continue to exercise both its Crisis Management and Crisis Communications Framework regularly against a variety of contemporary scenarios. The Review acknowledges that the AEC will do this from a position of strength.

Introduction

1. The *Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2018* received royal assent on 30 November 2018. The amendment required the Electoral Commissioner to establish a Transparency Register (the Register) as of 1 December 2018. The purpose of the Register is to make available to the public, information about political parties, significant third parties (previously political campaigners), associated entities, members of the House of Representatives (MPs), Senators, third parties, candidates, Senate groups, and donors registered with or recognised by the AEC.

2. The AEC established an interim Register on 1 December 2018 essentially by incorporating information from the Periodic Disclosure Tables, which had been published by the AEC since 2010. A major upgrade in October 2019 (and further upgrades in December 2019, February 2020 and November 2022) increased the Register's utility for users. The upgrade led to the inclusion of an address for entities at the top of each entity's banner. This caused the data breach for candidates, including current parliamentarians.

3. The Register provides public access through the AEC website to information the Electoral Act requires to be published, namely election returns and annual returns, including in some cases address data. The Register has incorporated data from the previously publicly available Periodic Disclosure Tables. Public access to the returns in those tables previously fulfilled some of the functions of the Register, including access to federal election returns since 1996.

4. The AEC's responsibility to have the Register, coexists with the responsibility to suppress the residential addresses of silent electors on the electoral roll. This is a statutory responsibility under s104 of the Electoral Act, which helps protect the personal safety of silent electors.

5. Silent elector status is important for candidates and parliamentarians as well as other members of the community such as survivors of domestic violence. In the case of parliamentarians, the AFP Commissioner Reece Kershaw told Senate Estimates on 31 May 2024 that in the past four years, reports of harassment, nuisance, and offensive and threatening communications, had increased 160 percent. There had been 725 reports to AFP to that point of the financial year.

6. On 15 May 2024, the AEC became aware of an inadvertent release of data on the Register, resulting in publication of 2680 election candidate residential addresses including the current silent addresses of 71 candidates, some of whom are serving parliamentarians. This occurred because of an AEC internal technical process error whereby the Register was automatically 'pulling' addresses from election candidate nomination forms to populate an address field in the entity banner for each candidate on the Register.

7. The error was not a cyber security breach. It did not otherwise impact the security, stability, integrity or functionality of the Register or any other AEC systems. The AEC took the Register offline as soon as the data breach was detected.

8. AEC's investigation of logs showed that of the 71 persons at highest risk from the breach, which included serving parliamentarians and other high-profile candidates, 17 actually had their entity banner with the address field viewed. The address fields of the other 54, while available for viewing, were never accessed. It should be noted, however, that the matter outlined at paragraph 11 below, means that other persons beyond the 17 whose address pages were viewed on the Register may have had their silent address accessed through the Register.

9. The AEC advised archived web pages from the Register were on the Australian National Library's (ANL) Trove website. ANL confirmed on 17 May 2024 that the pages had been archived and are no longer available for public viewing.

10. In addition to the impact on silent electors, some residential addresses for non-silent elector candidates were also drawn from candidate nomination forms and made available on the Register. While the addresses on the nomination forms were not provided to AEC for the purpose of publication, the same addresses would also have been publicly accessible on the electoral roll.

11. While investigating the breach, the AEC also detected another way that some residential addresses related to current silent electors could have been released onto the Register. The AEC is required by law to publish complete returns, which it does in PDF form, rather than being allowed just to extract and publish data from those forms. As a result, if a return provided to AEC inadvertently contained a silent elector address, or contained an address that later became silent, this address was published and remained published in the return on the Register. The issue has been treated as within scope of the Terms of Reference of this review. Its extent is under investigation by the AEC at the time of the Review's completion.

12. The Terms of Reference of the Review are made up of four questions. They dictate the structure of the Review which is divided into four broad sections titled:
    - How did this data breach occur?
    - What is the extent of the data breach?
    - Has the AEC remediated the issue to the best extent possible?
    - What lessons does the AEC need to implement to minimise the risk of similar breaches?

13. Each section, with varying focus and emphasis, focusses on both the technical/operational and governance aspects of the incident.

Term of Reference #1: How did this data breach occur?

14. To understand how this breach occurred, some background explanation on the Register is required.

What goes on the Transparency Register?

15. Since 2019, the AEC has published returns through the Register, which is accessible on the AEC website. The Register contains tens of thousands of entries.

16. AEC is required under s287N 287Q and 320 of the Electoral Act to publish the current register of entities, annual returns and election returns (detailed in Divisions 4, 5 and 5A), referendum returns, election funding claims and enforceable undertakings on the Register. Returns are provided by political parties, candidates, significant third parties, associated entities, Members of the House of Representatives, Senators, third parties, annual donors, Senate Groups, election donors, Referendum entities and Referendum donors, with each category having specific returns requirements. Returns are completed by filling out the relevant form approved by the Electoral Commissioner. Each category of return has its own information requirements.

17. In the case of the over 10,800 candidates[1] on the Register, the AEC is required only to publish election returns (and enforceable undertakings and financial claims if applicable). It is not required or empowered to publish candidate nomination forms on the Register.

What Addresses Were Used?

18. When the current Register was developed, the AEC included an address within the entity banner for each entity (including candidates). This was recorded in AEC working level project documentation as a 'user requirement'. It was not a requirement of legislation.

19. For most categories of entity on the Register, including an address was straightforward. The address field could be filled with publishable data from a return provided for inclusion on the Register.

20. Candidates' entries on the Register are somewhat different. For nominating candidates, the first address candidates provide to the AEC is likely to be on the nomination form, which is held on a separate IT system, the AEC Election Management System (ELMS). ELMS is an important IT system in the AEC, which is used for the detailed management of all electoral events.

21. Data from candidate nomination forms is also shared from ELMS with the AEC's Funding and Disclosure ICT system (FAD ICT system) for AEC administrative purposes. The FAD ICT system houses all returns. It too is an important AEC ICT system. The Register in turn draws its data and PDFs of returns from the FAD ICT system.

22. To populate its entity banner for candidates, the Register 'pulled' postal addresses from candidate nomination forms (or residential addresses as a fallback) from the FAD ICT system (see Appendix A). This was the primary reason for the data breach. It led to 2680 candidate nomination form addresses being published. In many cases, candidates did not consent to the address they provided being published. Most of the 2680 were not silent elector

[1] The Transparency Register 15 May 2024

addresses. 71 were current residential addresses of silent electors. AEC records show 17 of these were publicly viewed.

23. This Review has examined the project management and technical architecture documentation for the development of the Register. The development was technically described as an 'upgrade' within the AEC because information from the previously used Periodic Disclosure Tables was initially incorporated into an interim Register after the passage of relevant legislation in late 2018[2]. The Register's development then occurred under time pressure in 2019. It was treated as part of a larger 'Self-Service Platform' (SSP) project AEC was completing.

24. AEC intended that, unlike the predecessor Periodic Disclosure Tables, the upgraded Register would have a more user-friendly search function to enable better transparency. Searches by entity, including candidates, would be possible. Previously, public searches of AEC returns would require the searcher to know what return they were searching for to locate data.

How was it decided to include entity addresses on the Register?

25. The Review viewed low-level AEC project documentation for the Register which contained a 'user requirement' that an entity address be included on the Register. That was the extent of the documentation on the decision to have the entity address in the banner.

26. The risk of candidate addresses being drawn from the wrong system would not have been evident at 'user requirement' stage. The benefits of including an address were transparency and ease of entity identification. It was a logical decision. The presence of an address in the banner did not attract attention higher up within the AEC during the Register's development. This supports a finding that while the inclusion of addresses was unnecessary and regrettable, it was not unreasonable.

Finding 1: The inclusion of an entity address field in the Transparency Register from 2019 was unnecessary and regrettable, but in the context of a transparency measure, not unreasonable.

27. AEC records show that the Assistant Commissioner responsible for Funding and Disclosure, demonstrated the Register to the AEC Executive Leadership Team (ELT) meeting on 14 October 2019[3]. It is unclear whether this included a visualisation of a screen including a banner containing an address. If it did, it would likely have displayed a postal address, not a residential address, given the source of the data was a postal address field on candidate nomination forms. There is no documentation available to confirm this and it has not stuck in the memory of any of the participants interviewed.

28. The review concludes from paragraph 27 above that some ELT members may have known at least passively that an address was included in the banner of the Register. That an address was visible in the banner was unlikely to have been noteworthy because addresses are routinely provided for publication in returns. There would not have been any reason for senior AEC officers looking at a demonstration to think candidate addresses came from nomination forms.

---

[2] From October 2018 to October 2019 the Register did not include the problematic candidate nomination form postal addresses on entity banners.

[3] ELT minutes from 14 October 2019

29. There is no record of a decision in AEC documentation that the address to be included in the Register for candidates, would be drawn from their nomination form. The working level 'user requirement' to include an address was not prescriptive about where the address should come from. Additionally, the coding used by developers to make the address link between the Register and the postal address on candidate nomination forms in the FAD ICT system was at least ten years old.

30. This all indicates the decision to use those particular addresses for the Register was inadvertent, making use of existing computer coding in the FAD ICT system to deliver a convenient, quick technical outcome. The Review cannot be sure that speed and convenience were the reasons for those particular addresses being used, but words to this effect have been used by both mid and senior officers in the AEC to describe what they think happened and it is a reasonable conclusion in the absence of written proof.

31. Unfortunately, 'convenient' and 'quick' were not the ingredients for long-term success. The working-level technical decision to use candidate nomination form postal addresses to fulfil the user requirement was an error that should not have occurred. It led to the publishing of data not collected for that purpose and was the primary cause of the data breach.

32. Reflecting the lack of relevant detail in project governance documentation, the Review has been unable to attribute the decision to include candidate nomination form postal addresses on the Register, to any one person.

33. The Review has spoken to those whose names appear on the project documentation that still work at the AEC. They have been helpful and open but do not recall a decision to use postal addresses from nomination forms for the Register search result banner. Given the regular turnover of contracted staff working on ICT development since 2019, it is likely that those involved no longer work at AEC.

34. The Review can conclude from the documentation it has examined that those involved would not have envisaged the decision leading to silent elector addresses being published.

Finding 2: The AEC was wrong to publish postal addresses from candidate nomination forms in the Transparency Register entity address banners as those addresses were not collected for that purpose. It was the primary reason for the data breach.

35. The Review found nothing in higher level technical governance documents (i.e. Project Management Plan and project architecture documents for the SSP project) to indicate any senior-level knowledge of the undocumented working-level decision to populate the entity banner with candidate nomination form postal addresses.

36. It is perhaps stating the obvious that the governance around the decision was not sufficient.

Finding 3: Senior officers in the AEC were unaware of the undocumented working-level technical decision to include postal address data from candidate nomination forms in the entity banners on the Transparency Register. The governance around the erroneous decision was not sufficient.

37. After examination of documentation and interviews with many AEC staff at various levels (see Appendix B), the Review concludes it is not appropriate or feasible to assign blame or apportion responsibility to any individual or group of people in AEC for the data breach.

Unrelated data breach in 2019

38. The Review also sought details of an unrelated 2019 data breach at AEC where personal information of 938 candidates was briefly accessible in a document on the AEC's website for 15 hours. This involved a bug in an update to the Election Management System (ELMS) that prevented a data extract report from completely redacting some qualification checklist (a part of the candidate nomination form) contact data before it was published to the AEC website.

39. The 2019 data breach was swiftly remediated. The cause of that breach was different to the one in this Review, but two of its mitigations, one immediate and one longer term, are instructive.

40. As a result of the unrelated 2019 breach the AEC decided out of caution to remove the relevant candidate contact details from public view on the AEC website because they were not required by law to be published. This was seen as one way to mitigate against such a thing happening again and demonstrated the AEC's focus on risks to personal safety and privacy. The Executive Leadership Team (ELT) made that decision at a similar time to the Register 'going live'.

41. The ELT would have had no reason to think the existence of addresses in search result banners on the Register risked a similar outcome to the unrelated 2019 data breach. But what if it had it been asked to make a conscious decision about having candidate addresses in banners on the Register? Given the freshness of the 2019 breach in AEC corporate memory, it may well have taken the lesson of the 2019 breach and decided not to include addresses at all. This is posed as a hypothetical by the Review. The ELT was not asked that question. It might best be described as a 'sliding door' moment for the AEC.

42. The other relevant longer-term mitigation since 2016 is the maturing of the AEC's Privacy Management Plan (the Plan) which is a document in which AEC identifies its specific privacy management goals and maturity targets in accordance with Privacy Principle 1.2. (Footnote full text of APP1.2 here please.) It is overseen at First Assistant Commissioner level.

43. The Review has compared the AEC's 2018/19 Plan with its 2023/24 Plan. It is evident that since the 2019 breach, the AEC has demonstrated its awareness of its privacy maturity by judging itself more critically against its targets and setting itself a high bar in the way it protects personal and sensitive information – for relevant indicators the AEC actually marks itself lower on a three point scale of developing/defined/leader than it did in 2019 despite doing a better job.

44. The Deputy Electoral Commissioner advises that with the help of the Plan, the focus on privacy, and on not collecting, holding or publishing data unnecessarily has become a strong part of the AEC culture. The Review accepts that the AEC privacy and data management culture has improved significantly since 2019. The culture of 2019 cannot be examined or interviewed in the way documents and people respectively can to make a comparison, but based on what the Review has seen of the AEC of today, the evidence is persuasive.

45. The AEC is to be commended for this, but at the same time it must be asked why the 2024 issues with the Register were not found much sooner in an organisation with this culture.

Why wasn't the 2024 data breach found sooner?

46. The previous pages explain how the addresses came to be in entity banners on the Register. They do not explain how they were then able to sit on the Register for in some cases five

years, before being detected by an alert parliamentarian who noted their own 'silent' address appeared on the Register.

47. The lack of detection of the data breach until 2024 is likely the result of three factors. The first is that the only detected reference to an address field in the Register the Review could find was at 'user requirement'[4] level. It occurred early and was low down in the governance food-chain of the IT project. The formal governance documentation for the project did not specify that an address would be included in the search result banner of the Register, so there was no documented decision to be audited or reviewed, or any documented technical architecture to provide a roadmap to detect the breach.

48. The second connected factor is the lack of any identifying feature on the addresses. To know where the addresses came from, somebody auditing the system would have needed to examine the computer coding which sits invisibly behind the addresses. There was nothing visible that would flag an address to AEC staff members as being sensitive, short of them being personally familiar with a silent elector's address.

49. The third factor relates to the AEC's legislative authority to collect disclosure data and its legislative obligations to publish it. The Review assesses from discussion with AEC staff, that this may have led to the AEC not prioritising a focus on the Register when identifying privacy risks across the enterprise.

50. It could be argued that an AEC official familiar with the returns processes and timelines might by chance have viewed a particular entry in the Register and questioned from where in AEC an address had been drawn, but this is would have been good luck rather than a reasonable expectation.

Finding 4: **The lack of any formal documented decision to include an address in entity banners on the Transparency Register, and the junior level within AEC at which the inclusion of the address field was considered, contributed to the data breach remaining undetected for as long as it did.**

51. The inherent governance issues with the decision are dealt with later in the review.

52. Current and 2019 IT project governance are also compared later in the Review to draw conclusions about how well AEC has mitigated the risk of something similar happening again.

Could the data breach have been malicious?

53. The Review considered whether the data breach could have been the result of malicious intent. The Review found no evidence or suggestion of malicious behaviour. In addition, neither the technical architecture underlying the data breach, nor its impact, give cause for suspicion.

54. There is no basis for any finding of malicious intent.

A separate elector data release issue

55. In investigating the above breach, the AEC found a second, unconnected way in which silent elector data could be viewed in the Register. Unlike the discretionary publishing of candidate

[4] Transparency Register User Story 2365: Annual and Election Returns – Entity Details View, 7 August 2019.

postal addresses, which was not required by law, this second issue is a direct result of the legal requirement for AEC to publish returns. The AEC found it because when it was advised of the presence of the first silent elector address on the Register, it did not know the origin of it and examined the whole Register to identify potential sources of the breach.

Finding 5: In the course of the data breach investigation, AEC recognised the separate data release risk. Silent elector addresses had been inadvertently provided to the AEC, or had become silent after being provided, in returns published on the Transparency Register in accordance with *the Commonwealth Electoral Act 1918.*

What is this second issue that was discovered in the investigation of the data breach?

56. The Electoral Act requires not only that the data in specified returns is placed on the Register, but that the actual returns themselves be available on the Register. This occurs in PDF form. There is no mention in the Electoral Act of silent elector addresses being supressed on the Register. By way of contrast, the section of the Electoral Act dealing with declaration of nominations[5] says that a candidate's town or suburb is not declared if they are a silent elector.

57. This requirement to publish gives rise to two vulnerabilities which were identified in the investigation. The first is that if a silent elector inadvertently includes silent elector data on their return (notwithstanding prompts on the forms advising that the data will be published) then that address could not be amended, removed or redacted by AEC and would be viewable by a member of the public on the Register.

58. The second vulnerability is that if an entity who is not a silent elector includes an address on a publishable return and then subsequently became a silent elector, then the address they provided before becoming a silent elector could by law not be redacted from the original PDF and would be viewable on the Register.

59. AEC captures how many 'views' there have been of a candidate's entity banner, but not whether or how many times return PDFs or their contents have been accessed. The AEC must assume that some silent elector data has at some point been accessed from returns, but in the period of this Review, the AEC has not been able to advise how many entities on the Register may have been affected this way. It should be noted, however, that a fortuitous technical design element of the Register means that searching and accessing content from returns on the Register (as opposed to looking at a candidate's banner page on the Register) will not have in itself provided the searcher with the banner content[6].

60. Although the AEC had not focussed on the data release until it was recognised as part of the data breach investigation, the problem is not new. In theory at least, the problem existed already when returns were accessed through the Register's predecessor, the Periodic Disclosure Tables which were accessible from 2010-2018. Prior to that there was a web hosted solution containing PDFs of returns from 1996. From 1984 (when election funding provisions were incorporated into the Electoral Act) until 1996, any access to disclosure returns would only have been available in hardcopy.

---

[5] *Commonwealth Electoral Act 1918* s176(1) and 176(3).

[6] Meeting on 3 July 2024 with Disclosure and Compliance Assistant Director, FAD ICT System Project Coordinator and FAD ICT System Test Analyst.

How did this happen?

61. In one respect, explaining how it was possible the public could access silent elector addresses from returns is simple. The AEC was doing its job. In accordance with the Electoral Act, the Electoral Commissioner approves forms to be filled out to lodge a return. The forms request an address (in some cases by law) which the AEC requires to perform its functions. The Electoral Act requires the returns themselves, not just data from them, to be published.

62. Apart from the legislative requirements related to the Register, however, the AEC also has a legislative requirement to suppress silent elector addresses on the Electoral Roll. These two requirements are in apparent conflict in relation to the requirement to publish returns in full. Those returns may contain silent elector information that the Electoral Act gives no power to the AEC to redact, remove or amend.

63. The AEC's obligation and ability to suppress silent elector addresses have their limits. The AEC makes clear on its website that granting a request for silent elector status, will not cause an address to be suppressed on historical electoral rolls, which may exist outside the AEC. This is a reasonable and realistic position for the AEC to take. It is responsible for data it holds and publishes but cannot be responsible for historical data which may have been legitimately previously accessed by an external party or which otherwise exists outside the AEC.

64. Those limits do not extend to the Register. There is nothing in the Electoral Act or in the explanatory memorandum for the *Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Act 2018*, which indicates any willingness or intent for silent elector data to be published on the Register by AEC. Interpreting matters of law is not the role of this Review, but it is reasonable to conclude that the publication on the Register of silent elector addresses in returns was not an intended consequence of legislation.

Why wasn't this data release detected sooner?

65. The Review considered why the AEC had not previously focussed on this data release prior to discovering the breach in May 2024.

66. Silent elector addresses on the electoral roll are diligently protected within the agency. Only a relatively small number of staff have access. The agency takes its cyber security and compartmentalisation seriously, and the AEC's Roll Operations and Silent Cell works to strict protocols to preserve the security of the silent elector data. Silent elector information is held securely within the AEC systems and detail is only displayed to staff with the appropriate access. This access is reviewed at regular intervals to ensure the small cohort of staff that have access remains current and accurate.

67. When an elector's data is supressed on the roll, it is also automatically supressed in other AEC systems where the elector's name and electoral roll address appear together. This automatic suppression does not extend to return PDFs or other places where the elector's name and silent address may appear together, but where the address had been provided by the candidate either without highlighting that it is a silent address, or before it became a silent address. An automated solution may still be some years away. In the meantime, the AEC needs to understand everywhere in its systems silent elector addresses might reside.

68. The careful separation of the silent elector function within AEC contributed to a vulnerability in respect of the data release. Because silent elector addresses are carefully compartmented and protected within the agency, and the relevant data in the returns on the Register was not

identifiable as silent elector data, the risk of disclosure of silent elector data from historical PDFs was not identified or actioned by AEC at enterprise or technical level.

69. It was during the data breach investigation the AEC recognised the data release risk that existed in relation to returns on the Register. The AEC temporarily remediated the PDF silent elector data release issue at the same time as remediated the data breach, by bringing down the Register. It took this cautious measure without knowing the extent of the data release.

Finding 6: The AEC temporarily remediated the separate data release risk in Finding 5 at the same time as it remediated the data breach, by taking the Transparency Register offline. How many silent addresses were in published returns and whether they were accessed is not known at the time of the Review.

70. The Review strongly endorses the remediation measure the AEC took. While it acknowledges that historical documents containing now silent addresses exist outside the AEC, would be a different matter for the AEC itself to provide ongoing public access to historical data which included current silent elector addresses.

Recommendation 1: That the AEC audit those of its systems which do not automatically supress silent elector addresses, so it is positioned to identify, and where necessary supress, any silent elector addresses present on those systems.

Governance

71. In explaining how the breach happened, the Review also examined the governance over projects and IT systems in AEC in and around 2019.

72. An interim version of the Register was brought online in 2018, replacing the existing Periodic Disclosure Tables. Within a year, in October 2019, the upgraded Transparency Register went 'live' as a deliverable of the Self-Service Portal project the AEC was undertaking. Only this final version included the field that in some cases contained silent elector addresses.

73. Further minor Register upgrades occurred in December 2019 and February 2020. A global search function was added in November 2022, which among other things, meant that a candidate and their address would appear on the Register before they furnished any returns.

74. The speed with which the Register was developed reflected legislative requirements to have a Register, to deliver a better 'user interface' as part of the capability as quickly as possible.

75. The Review has examined the Project Management Plan and the 2019 Transparency Website Design documents for the Register[7]. The documentation looks professional as far as it goes but does not provide detail in relation to the problem issues described in this Review. The Register project documents from 2019 only mention the user requirement for an address field in the Register in the 'user story', which is a low-level project document. The project documents also do not mention using postal addresses from candidate nomination forms.

76. In any event, the governance of the Register above that level was also lacking. The development of the upgraded Register in 2019 was included in the AEC's bigger SSP project, which was already underway. The SSP had a Project Board chaired at First Assistant

[7] Self-Service Platform Project Management Plan Version 1.5, 17 May 2019 and Self-Service Platform Transparency Website Design, 30 September 2019

Commissioner level and a detailed project management plan. It does not appear in retrospect from that documentation in 2019 (or from discussion with one of the SSP board members of the time) that the Register was adequately integrated into the governance work of the Board.

77. Given that detailed consideration of the Register development was apparently not occurring at Project Board level, it is unrealistic to think that in 2019 these matters would have been surfaced or decided anywhere higher in the organisation's then governance structure such as the Capability Committee headed by the First Assistant Commissioner Capability, or the Executive Leadership Team headed by the Electoral Commissioner.

What Was the Theoretical Governance over the project in 2019?

78. The extent of overarching ICT project governance documentation in 2019 appears to have been the Project Engagement Model v1.0 of 25 July 2018, which was heavily based on PRINCE2 (a project management methodology). Above that, the AEC had a 2018-2022 IT Strategic Plan. The Review could not see any obvious faults with the documents but was not left with a sense of confidence about the robustness of the overarching ICT governance documentation in 2019.

79. The Review asked relevant First Assistant Commissioners their recollections and views on this. One advised the Review that 'Agile' project management processes were still new to the AEC at that time and the AEC project governance structure did not have experience with them. The maturity of the organisation to govern an Agile project was low.

80. Once the Register content and architecture that allowed the data breach was in place in late 2019, the lack of any external complaint about the presence of addresses or any internal concern about the Register's published content, meant the chances of detection of the data breach (or the data release) were not high.

81. Updated governance documentation was definitely in existence in 2021. It is evident to the Reivew that the governance of ICT projects since that time has improved significantly in the AEC (this is discussed in detail later in the report).

82. While website maintenance and curation are a downstream issue, it is evident from discussion with Branch heads responsible for Disclosure and for Enterprise Digital Delivery that there is not perfect clarity in AEC about ongoing roles and responsibilities in respect of website maintenance and curation as it relates to the Register.

83. It is important for the AEC that business owners are regularly reviewing their website content. The CIO Division is an enabler within AEC, but should not be curating the information within public facing applications. Given the breadth of public facing 'surface area' the AEC administers, there is a recommendation below in relation to maintenance and curation.

Recommendation 2: That AEC review its management of website and Transparency Register maintenance and curation, to ensure these roles and responsibilities are clear across the organisation.

84. Current 2024 ICT governance in AEC is contrasted with 2019 later in the Review to enable judgements about mitigations and recommendations in relation to governance.

Term of Reference #2: What is the extent of the Data Breach?

The statistics

85. To examine the extent of the breach it is necessary first to put the data breach in perspective.

86. There are tens of thousands of entries on the Register, including over 15,000 candidate entries for over 10,800 persons (some have multiple entries).

87. A total of 2,680 candidates, including parliamentarians and past parliamentarians, were technically affected by the data breach as the residential address published with their name on the entity banner on the Register was not collected for that purpose.

88. Of those 2,680, 311 were silent electors. Of those, only 71 were considered to be at high risk because their current silent residential address was published. That number can be qualified further because the entries of only 17 of that 71 were actually publicly viewed.[8]

89. The AEC has a comprehensive framework of enterprise level risk governance documentation discussed later in the report. The Review applied the AEC's current 'Risk Management and Consequence Table'[9] to conclude the risk consequence of a data breach of this extent sat at 'major', which is the second highest level. Of the seven headings against which consequence is assessed in the table, one is Privacy which is defined as:

> *'Sensitive information accessed/ disclosed, including of high-risk individuals. Potential serious risk of harm to individuals. Requires assessment as an 'eligible data breach' under the Data Breach Response Plan. Potential for major loss of public confidence.'*

This is a reasonable description of the extent of what the AEC faced prior to its remediation and mitigation efforts; a conclusion supported by the fact the AEC assessed what occurred as an 'eligible data breach' in accordance with the *Privacy Act 1988***.**

90. The Review has defined "extent" broadly to include not just the number of people impacted, but also impact on personal safety, privacy, and public confidence in the AEC's protection of data.

Personal Safety

91. The AEC approves silent elector status based on a risk to personal safety[10]. The most serious impact of the data breach would be an incident that endangers personal safety. This impact was examined through discussion with AFP, which assisted the Review at Assistant Commissioner level.

92. Without making public anything sensitive about security and law enforcement agencies' operational posture, the AEC's and AFP's immediate focus was on the 71 individuals whose

[8] This figure of 17 does not include those entities whose current silent elector address has been provided to the AEC in a published return that may subsequently have been publicly viewed.

[9] August 2023 AEC Risk Management and Consequence Table.

[10] Silent electors - Australian Electoral Commission (aec.gov.au)

current silent elector address had been published and who were therefore at greatest risk of serious harm.

93. The AFP advised the Review on 19 June 2024 that it had not detected any security incidents resulting from the data breach. This is obviously a 'point in time' assessment. The AFP cannot discount a future security incident but credits the AEC's swift and effective communication with the AFP and the multi-agency Security Coordination Committee (SCC) it leads, as having lowered the operational risk of an incident.

94. The AFP, supported by other the agencies on the SCC, which includes in its number the Department of Home Affairs, Department of Parliamentary Services, Department of Finance, Department of Foreign Affairs and Trade, Department of Defence and Department of the Prime Minister and Cabinet, has taken account of the information provided by the AEC for its risk assessments and operational posture as it continues to monitor for any sign that the data breach could lead to a threat to physical security.

Finding 7: That 2680 candidates were technically affected by the data breach. For the vast majority the breach had no practical impact. For 71 individuals the breach caused a potentially serious risk to personal safety. The addresses of only 17 of the 71 were actually viewed as a result of the data breach. This figure of 17 does not account for any current silent addresses provided in returns on the Transparency Register ("the data release") that may have been publicly accessed.

Finding 8: Based on consultation with the Australian Federal Police, the Review finds that the incident response, mitigation and communication steps taken by the AEC upon discovery of the data breach, lowered the risk to personal safety of the data breach.

Finding 9: Based on advice from the Australian Federal Police the review finds that there has not been any personal safety impact from the data breach at the time of writing. This is necessarily a point in time finding only.

Privacy

95. Ultimately any formal judgement about the impact on privacy of the data breach is a matter for the Office of the Australian Information Commissioner (OAIC). The Review can only give a commonsense, point-in-time view.

96. Given the public profile of the most affected individuals, the sensitivity of the personal information involved (residential address) and the public nature of the disclosure, the AEC formally reported the incident to the OAIC as an Eligible Data Breach under the Notifiable Data Breaches Scheme on 22 July 2024.

97. In the lead-up to this, the AEC first contacted the OAIC to outline what had occurred on the morning of 15 May 2024 when the data breach was discovered. It also contacted 22 persons assessed to be at high risk from the data breach on that day. AEC wrote again to those at high risk on 17 May as well as a further 54 impacted persons. On 24 May 2024 AEC provided formal data breach notification to those at high risk impacted by the data breach (with OAIC advised this had occurred on 28 May). All others impacted were informed by the publication of a 'Notification Under the Privacy Act 1988' on 24 June 2024.

98. Further refinement of the number of people most impacted occurred in the ensuing days. The most impacted 71 people in a privacy context were parliamentarians, past parliamentarians and high-profile candidates who had been assessed by AEC, either while in parliament or

prior to that, as having a valid reason to be a silent elector. The entity banners of 17 of those 71 were actually publicly accessed. These persons would have assumed the AEC would not publish the address from their candidate nomination form on the Register and that they could depend upon the suppression of their address as a result of being a silent elector.

99. Whether the breach or the separate data release issue have had a specific privacy impact on any of the 17 beyond the publication of the addresses and the concern this has caused, is not evident to this point. This may only be known over time. The AEC had communications with the 71 affected individuals, the AFP and the OAIC. None have indicated any specific impacts on an individual as a result of the privacy breach to date. The principle that the personal information from candidate nomination forms should not have been published remains.

100. While the personal information for the remainder of the 2680 affected candidates should also not have been published, the potential for further specific privacy impact on them cannot be compared to the 17 as the remainder were either not currently silent electors (the vast majority), did not have their current silent address published or did not have their published silent address viewed as a result of the breach.

101. The Review discussed the AEC's handling of the data breach to date with the Acting Deputy Commissioner at the OAIC, Melanie Drayton and Assistant Commissioner Dispute Resolution, Andrew Castaldi on 21 July 2024. The Review explained its relevant provisional recommendations and findings. The OAIC officials outlined the processes to be followed by AEC in reporting and mitigating the notifiable data breach. The OAIC subsequently confirmed that the AEC had met its reporting obligations under the Privacy Act 1988.

Finding 10: Based on consultation with the Office of the Privacy Commissioner, the Review finds that the AEC has met its privacy responsibilities to the Australian Information Commissioner and the public in the way it has communicated the notifiable data breach and provided information about it.

Reputation

102. With 17 individuals potentially seriously impacted by the data breach and 2663 others technically affected, the extent of its impact on the reputation of the AEC is examined briefly below.

103. The AEC is an essential component of Australia's democratic system. It delivers free and franchised elections. As such, confidence in its ability to manage the security, integrity and access to information is of the highest importance.

104. The AEC takes management of its reputation very seriously. It has a formal Reputation Management System accessible on its website. It explicitly links trust in the AEC to trust in the Australian Electoral processes and results. It includes specified areas of operational excellence, key principles and the AEC's values[11].

105. AEC itself said in its privacy breach notification of 24 June 2024:

> *The AEC takes enormous pride in its reputation as a world-leading electoral management body. Privacy is among our highest priorities. This is a deeply regrettable situation, for which we sincerely apologise.*

[11] The AEC Reputation Management System - Australian Electoral Commission

106. A consistent theme from meetings with AEC senior officials is that the AEC sets itself a high bar in terms of the security and integrity of its data and the resilience of its systems. It is comparatively well trusted among public service agencies. For example, the APSC's 2023 Trust in Australian Public Services report found that 91% of Australians trust the AEC – the highest level of trust across all public service agencies.

107. The public reaction to the AEC data breach has to this point been restrained. There has been some media coverage, but it has not been extensive or critical. There has been communication between the AEC and impacted persons (current and past parliamentarians and candidates). This has included understandable concern and questions about what has occurred from some of those impacted, as well as praise for how the AEC is handling it from some others. There have been no obvious signs of public anger or frustration other than questions about when the Register would be back online. (As of 25 July 2024 the Register was back online without addresses in the entity banners and without PDFs of original returns.)

108. Regardless of the initial reaction, the AEC must work on the basis that its reputation for secure information management has suffered publicly to some extent as a result of what has occurred. The two factors that will impact reputation from here on are: the AEC's ongoing management of the data breach; and whether there are any actual personal safety or further specific privacy impacts.

109. These are, of course, only point in time observations by the Review.

110. To this point, the AEC's management of the data breach has demonstrated transparency and good communication, timeliness, effective remediation and mitigation (see Term of Reference 3 below). This will assist it to build and maintain its reputation.

111. Whether any personal safety or further specific privacy impacts eventuate is partially beyond the AEC's control. Its good communication with the AFP and agencies that support it on the SCC, and with the OAIC, have helped minimise those risks and the impact they have had on the AEC's reputation.

112. There is also a potential reputational impact on the AEC as a result of taking the Register offline. The Register plays an important role in providing transparency of political financing. It is an important element of our democratic process and it helps protect against foreign interference. It is required of AEC by the Electoral Act.

113. The AEC had a number of enquiries from the media and academics since it was taken offline asking when it would be available again. This is only one indicator of its value. The AEC recognised that the longer it stayed offline the greater the risk to its reputation from a transparency perspective.

Finding 11: It is unavoidable that the data breach will have had some impact on the AEC's strong reputation for securely managing information. Its ongoing actions since the data breach will help minimise that impact.

Extent of separate silent elector data release issue - more silent addresses on the Register?

114. The extent of the separate silent elector data release issue discovered during the investigation of the data breach is the more difficult to determine the extent of, because there is less data available.

115. To recap, this second issue was the AEC's recognition during the data breach investigation of the risk that there were some silent elector addresses on returns themselves.

116. Returns must be published on the Register by law. It is clear on the approved forms which entities complete to lodge a return, that the completed return will be published on the Register. A silent elector address can be erroneously provided in a return by an entity. An address can also become silent at some point after being legitimately provided by entity as a non-silent address. In either case, once provided, it remained on the Register under current legislation.

117. This data release issue is unrelated to the data breach and it is not a cyber security breach. It is the result of the legal requirement that AEC publish returns on the Register. Nevertheless, it has the potential to cause the same risk to personal safety for an affected individual as the data breach.

118. The AEC cannot quantify the extent of this silent elector data access issue in the way it can with the data breach. As a temporary measure it remediated the issue by taking the Register offline. While the Register was offline, the AEC identified 1251 returns on the Register that were provided by, or which named, high-risk silent electors affected by the data breach.

119. While the identification of 1251 returns belonging to silent elector candidates is an important step, it does not provide a guarantee that there were not further silent elector addresses provided in the tens of thousands of other entries that were accessible on the Register. Although the approved forms filled out to lodge returns make clear they will be published, the AEC assesses that there has been erroneous inclusion by entities of silent elector addresses, and inclusion of legitimately provided addresses which have subsequently become silent.

120. In the time period of the Review, the AEC was not in a position to provide further data on silent elector addresses that may be present on the Register. Proposed longer-term remediation to provide assurance that no silent elector addresses can be returned to the Register is offered at Recommendations 5 and 6 under Term of Reference 3. The action the AEC has taken in putting the Register back online on 25 July without PDFs of original returns and without addresses in the entity banners is consistent in outcome with what is proposed in the recommendations.

Personal safety and privacy impacts

121. The personal safety and privacy impacts for those considered at high risk in the data breach do not change as a result the silent elector data access issue. However, the Review must conclude based on what advice AEC has been able to provide about the data release, that the silent elector addresses of some additional entities were accessible (though not necessarily accessed) on the Register, which could lead to an increased personal safety risk for them.

122. Subsequent to briefing the SCC on the data breach, the AEC also briefed the AFP on the data release at AEC First Assistant Commissioner to AFP Asisstant Commissioner level. At the time of the Review the AEC is considering whether there are any further steps it could take which would minimise the risk to any person whose silent address was on the Register in the data release.

123. The data release is not a data breach. The AEC was publishing what it was obliged to by law, so there is no apparent obligation for anything further to be reported formally to the OAIC. Nevertheless, the data release issue does have potential for practical privacy impacts on affected individuals even though the data was lawfully published. Any impacts would only be known in time and cannot be quantified.

Reputation impact of the data release issue

124. The potential impact on the reputation of the AEC as a result of the data release issue cannot be discounted but should not be considered in the same light as for the data breach. In this instance, the Electoral Act requires the AEC to publish returns on the Register and the addresses provided to the AEC in returns are provided for the purpose of publication.

125. Any silent elector addresses within the returns are either the result of error on the part of the provider of the address, or because an address has become silent after being provided. In either circumstance the AEC does not have a legal basis to remove the address from the Register. While this issue requires permanent remediation, and ideally would have been identified long before 2024, the Review does not consider it to be the fault of the AEC in the way the data breach is.

126. The extent of the impact on the reputation of the AEC of this data release issue is unknown at this time as the issue was only recognised in the course of the investigation of the data breach. But noting the AEC:
    - was meeting its legal obligations in publishing returns;
    - has responded transparently by encouraging inclusion of the issue in the terms of the reference of this Review;
    - and quickly temporarily remediated the risk at the same time it remediated the data breach,

    there is reason for AEC to be cautiously optimistic it should not have any significant reputational impact. This is a point-in-time judgement, which is all the review can offer based on the information available.

127. Clear communication and remediation will help the AEC maintain its reputation in relation to this issue.

Term of Reference #3: Has the AEC remediated the issue to the best extent possible?

128. In examining AEC's remediation of the issue, the Review has considered remediation of both the data breach, and the separate data release issue discovered during the course of its investigation of the data breach. The Review has also taken the liberty of including mitigation in its definition of remediation to providing an understanding of AEC's response.

129. This Review considers remediation in respect of immediate incident response, including communication, technical response and longer-term measures.

Immediate incident response and communication

130. The AEC became aware there was an apparent data breach at 0900 hours on 15 May 2024 through a call from the office of the Special Minister of State, the Hon Don Farrell MP, advising that a parliamentarian had notified the office that their residential address was displayed on the Register.

131. AEC's Executive Leadership Team was briefed in the following 90 minutes and the organisation had convened an Incident Management Team (IMT) in accordance with its crisis arrangements by 1200 hours.

132. By 1345 hours on 15 May the Register had been taken offline. By that evening the AEC had contacted the first two persons identified as impacted by the data breach. The AEC also provided initial advice to the OAIC that evening and attended an AFP-chaired multi-agency SCC meeting at AEC First Assistant Commissioner level.

133. Later in the evening of 15 May AEC advised a further 20 persons assessed at that point to be at high risk by email that their silent elector addresses had been published (these 22 as well as a further 54 persons were emailed again on 17 May).

134. As a precaution, the AEC also provided advice to the Special Minister of State, the Hon Don Farrell MP, Shadow Special Minister of State, Senator Jane Hume, Political Parties' Deputy Registered Officers, Department of Finance, the Attorney-General's Department, Electoral Integrity Assurance Taskforce, the Australian Cyber Security Centre, the Australian Taxation Office, the Australian Prudential Regulation Authority, the Australian Securities and Investments Commission and States and Territories Electoral Bodies.

135. The IMT continued to meet regularly, and the AEC Communications team worked closely with it, using the AEC approved 'Communications Response Plan template – Potential Data Breach'[12]. By early afternoon on 16 May the AEC had concluded it had remediated the data breach and issued a media statement.

136. A chronology of the AEC's initial response actions is attached in the document at Appendix C.

[12] 30 April 2024

Incident response governance

137. In looking at the effectiveness of the outcome of the actions above, the Review also considered the management and governance sitting behind the response.

138. The AEC Incident and Crisis Management Framework (ICMF)[13] is the framework that governed the incident response to the publication of silent elector addresses.

139. The ICMF outlines six stages of AEC's incident and crisis management process: plan and prepare; incident and initial response; assess, communicate and escalate; manage/respond; resolve and communicate; and review and improve. The AEC has done or is doing those things.

140. The Review considered the content of the ICMF, interviewed the National Incident Manager (NIM), First Assistant Commissioner Michael Lynch and the Assistant Commissioner Communications, Education and Engagement Branch, Cathie Kennedy, and inspected sample minutes of the 16 IMT meetings that occurred between 15 May and 18 June 2024.

141. The review concluded that the Framework was well constructed as a fit-for-purpose crisis/incident response document for the AEC. It has a clear link to the Australian Government Crisis Management Framework, and it had been used for exercise/training purposes to rehearse incidents and crises in the lead up to the discovery of the data breach. Most importantly, AEC used it to guide its response.

142. The Communications Response Plan template – Potential Data Breach and the External Incident and Crisis Communications Framework[14], which had been tested in an AEC exercise recently also served the AEC well in an environment where communication was essential while an understanding of the data breach was still unfolding.

143. The Review concludes that the decision by the IMT to treat the matter as an 'incident' and not a 'crisis' in accordance with the ICMF was appropriate, was regularly reviewed, and accorded with the AEC's own definitions in its ICMF.

144. The timeliness of the advice to the Electoral Commissioner and Deputy Electoral Commissioner aided decision-making and ensured the Register was taken offline within five hours.

145. For the longer-term investigation effort the data breach required, the AEC formed an Escalation Cell made up of subject matter experts who are highly respected staff in the AEC. Picking a fit-for-purpose team worked well to develop a taxonomy of the data breach and to identify the data release issue.

146. Consultation with other agencies was well managed by the NIM in response to this incident, but occurred based on his own judgement that it was needed, not on explicit guidance in the ICMF documentation. This gives rise to Recommendation 3 below.

147. The above is an endorsement from the Review of the AEC's Crisis/Incident Management arrangements, and how they have been used in this case.

---

[13] V1.3 of 29 August 2023

[14] March 2024

Recommendation 3: That the AEC's Crisis and Incident Management doctrine include explicit guidance on consultation with other agencies.

Finding 12: The AEC Incident and Crisis Management Framework, which governed the incident response is well constructed, connected to broader Commonwealth government crisis arrangements and was effectively implemented. This contributed to the swift remediation of the data breach and risks it presented.

Technical response

148. The key element of the short-term technical response was AEC's quick decision to take the Register offline. This was a decision warranted by the incident the AEC was facing and provided an immediate, and it appears complete, temporary remediation of the ongoing technical risk. Because the data release issue discovered during the investigation also involved data publicly available only through the Register, this too was remediated in the short-term by the Register being taken offline.

149. The short-term technical threat posed by the data breach and data release has been remediated to the best extent possible.

150. In making the decision to take the Register offline, the Electoral Commissioner had to consider the AEC's legislative obligation to have a Register. He also had to consider the prospect that leaving it online could increase the personal safety risk for some silent electors, the suppression of whose residential addresses on the Electoral Roll is also a legislative obligation for the AEC. The Electoral Commissioner, Tom Rogers and Deputy Electoral Commissioner, Jeff Pope, both told the Review that keeping the Register online in the current form was not tenable.

Finding 13: The Electoral Commissioner took the only viable course of action to achieve short-term technical remediation of the publishing of silent elector addresses by taking the Transparency Register offline.

Longer term remediation

151. The Review has also examined the longer-term technical remediation effort. For the data breach, the approach has been to remove the entity address field from the search result banner for each entity on the Register. The address in the search result banner was never required by the Electoral Act, so this solution requires no legislative amendment. It can also be quickly technically achieved, to ensure the breach cannot be repeated.

Recommendation 4: The Review recommends that the AEC remove addresses from Transparency Register entity banners.

152. The more difficult longer-term remediation related to the data release issue. The Register provides access to tens of thousands of returns from the AEC Funding and Disclosures database (the FAD ICT system) that must be published in PDF form to meet the requirements of the Electoral Act.

153. As noted above, at the time of writing the AEC had identified 1251 returns as having been provided by or naming candidates considered to be at highest risk from the data breach. This is an important risk mitigation for those judged at highest risk, but it is not sufficient remediation as it does not account for addresses of other silent elector addresses that may be on returns that were accessible on the Register.

154. During its investigation of the data breach, the AEC has, as explained above, recognised an ongoing risk associated with its legislation, which currently requires returns themselves to be published on the Register (and not simply data extracted from returns).

155. The Review finds that for long-term remediation of the data release, not only does the address field need to be removed from entity banner page, but the AEC should also recommend to government and the Department of Finance a legislative amendment to the Electoral Act.

156. The legislation should be amended such that the Register requires only content from returns, not returns themselves, to be published on the Register. This will permanently remediate the data release issue and allow the AEC to meet its legislative obligation to put the Register back online, without any silent elector addresses present. The legislative amendment should include the power to remove, redact or amend information and cover all historical returns and information provided prior to the amendment. This should not be taken to mean that all historical instances of silent elector addresses outside the AEC will be protected.

157. This legislative amendment would provide the basis for AEC to do what needs to be done to protect Silent Elector addresses in returns from being published on the Register. The job of making sure these silent elector addresses are actually redacted or removed from the Register will regardless still needs to be technically achieved.

158. The AEC has delivered a solution for this in advance of potential legislative amendment. On 25 July 2024 it put the Register back online without the original PDFs themselves being included. This has remediated future risk (though not the ongoing risk from past accessibility) of silent elector addresses being accessible from PDFs of returns, while once again giving the public access to the Register. The Review supports this step, noting it has at least temporarily achieved the outcome proposed in Recommendation 6.

Recommendation 5: That the AEC recommends to government and the Department of Finance an amendment to the *Commonwealth Electoral Act 1918*, which requires publication of returns information rather than publication of returns. The amendment should also give AEC the power to redact, remove or amend information on the Transparency Register including past returns and information provided prior to the amendment coming into effect.

Recommendation 6: That the AEC redact or remove silent elector addresses prior to putting the Transparency Register back online.

Can AEC provide protection of silent elector addresses that exist outside AEC?

159. Some silent elector addresses will continue to exist on historical AEC documents that reside outside AEC. This is not a new revelation and the AEC has been explicit on its website that when it suppresses an address on the Electoral Roll it cannot guarantee its suppression on historical documents. The Review concludes from discussion with AEC officials that there is not a feasible remediation that can be proposed in relation to all documents that may exist outside the AEC.

Electoral Commissioner's approved forms

160. Recommendation 5 would in theory alleviate the need for a recommendation to review the content requested on the Electoral Commissioner's approved forms.[15] The Review prefers a cautious approach in line with the AEC's professed prioritisation of privacy.

161. Under the current legislation, a form approved by the Electoral Commissioner becomes 'a return' on the Register after being filled out. Addresses requested on an approved form by law or for AEC's functions had to be published on the Register. It follows that the AEC should ensure maximum discipline in requesting only the information that it needs to collect, and that information is collected in a way that protects that which is not to be published. As a matter of good governance, the Review recommends:

Recommendation 7: That the Electoral Commissioner review the 'approved forms' for returns on the Transparency Register to ensure the forms seek only the information required by the *Commonwealth Electoral Act 1918*.

162. At the time of writing the Review understands that an AEC review of approved forms which collect personal information, has just commenced.

Communication as a mitigation

163. The significance of the AEC's communication in remediating the incident is also worthy of mention. The AEC has received positive feedback from candidates about its good communication with impacted silent electors. It has also received feedback from candidates expressing understandable concern about what has occurred. The AEC thus far has been committed in its efforts to keep those affected informed. This work needs to be ongoing, particularly with those who have been assessed as in the high-risk category.

Finding 14: The AEC should continue its work in communicating personally with those who have been affected by the data breach or data release and are assessed to be at high risk.

164. The second aspect of the mitigation lies with the AEC's relationship with the AFP and the agencies that support AFP on the SCC. By advising the SCC what addresses may have been viewed in the data breach, it positioned the AFP with the support of others, to feed that information into risk assessment processes for their operational purposes to minimise the risk to personal safety for the impacted silent electors. This mitigation will be relevant for as long as AFP and other agencies on the SCC decide.

165. Exposure of silent elector addresses should also be placed into broader context. The Review will not articulate them, but there are always other ways a silent elector's address could become publicly known that have nothing to do with the AEC or silent elector status. As a result, a complete or permanent remediation is beyond the powers of the AEC or the AFP and agencies that support it.

Finding 15: The AEC has remediated both the data breach and data release issue to the best extent possible to this point. Remediation, risk mitigation and communications work are ongoing and, in some areas, subject to acceptance of the Review's recommendations.

[15] Section 4(1) of the *Commonwealth Electoral Act refers to approved forms*.

Term of Reference #4: What lessons does the AEC need to implement to minimise the risk of similar breaches in the future?

166. The findings in the previous Terms of Reference inform and, in some cases, specify what lessons (or actions) the AEC needs to implement to minimise the risk of a similar breach in future. Importantly the Review has found that some of the most important lessons have already been, or are being, implemented since 2019. Specifically, without reference to the data breach, the AEC has significantly improved its risk management framework and project management and governance.

Risk management and project management and governance

167. Risk management, and particularly project management and governance are the areas where implementation of lessons learned is most important for AEC in minimising the risk of similar breaches.

168. Adherence to the AEC Risk Management Framework and improved ICT project management will help the organisation to minimise the risk of similar future breaches.

169. The Review has examined the 2019 Risk Management Framework, which was comprehensive in structure, and included a Risk Management Policy and Handbook, Risk Appetite Statement, Risk Register and Risk Matrix and Escalation Table.

170. The 2019 risk documentation itself was satisfactory at a high level, in that it highlighted the likelihood and consequence of a data breach in the 2019 Risk Register, and the policy documents showed where project management risks should be considered. The 2019 Risk Register itself, however, was repetitive and would have required refinement to have been valuable to high-level committees. (A more strategic AEC risk document is referenced at paragraph 172 below.)

171. Among the 236 risks on the 2019 Risk Register were two which were very similar and relevant to data breaches and included between them, “compromise of information stored on an ICT system; …accidental release of information …; ineffective information management; and processes are not followed.”

172. Elements of these two risks both broadly envisaged a data breach of the type discovered in 2024 (as well as other types of risk events). The overall residual risk rating for both was “medium”. They did not stand out. The risk consequences in both include “a privacy breach” among other text. Personal safety was not referenced as a consequence against either risk.

173. In July 2019 the ELT approved a strategic and enterprise risk statement that succinctly articulated five risks at that level. The second risk included a risk impact of a ‘privacy or confidentiality breach’. Personal safety was again not referenced.

174. The Review also considered what lessons needed to be implemented in relation to working level identification and elevation of risk. In 2019 the risk of including an address in the entity banners on the Register, and that address being pulled from candidate nomination forms, was not identified at working level. It was therefore not elevated even to the SSP Project Board (which technically oversaw the development of the Register) for decision.

175. There is no record that there was any level-appropriate mandatory training dedicated to risk identification or risk management in 2019. Given also that the Risk Register content did not have relevant risk issues 'up in lights' it is quite possible that the risks that caused the data breach would not have been at the forefront of working level officer's minds.

176. This raises two questions for the present day. In 2024 are AEC staff at EL1 (the lowest level of management) and below, adequately informed in identification of risks in accordance with the 2023 AEC Risk Management Handbook?

177. The Review has observed that the 'risk awareness' shown by staff members it has met at all levels appears to be high. The risk management training modules available to staff also provide a good basis for training, though they are not currently mandatory (apart from a brief introduction in the AEC's National Induction Program). The Review finds more could be done in this regard to give greater assurance to AEC. After discussion with the Assistant Commissioner responsible for risk and business continuity and with his staff, the Review finds as follows:

Finding 16: That a brief module on risk management that recognises the expectations at different work levels, be incorporated into the AEC Mandatory Learning Program to provide further assurance to AEC.

178. The second question is, would a technical risk of the type that caused the data breach be visible in the organisation in 2024 such that action could be taken? To answer this the Review examined the entirety of the AEC's extant 2023 risk management framework documentation and met with both SES and working level staff to discuss project management and governance in relation to the AEC's biggest current project, 'Program Indigo'. Indigo is a once in a generation, multi-phased, multi-year program to transform the engines of democracy and how the AEC delivers electoral services, ensuring the needs of voters are met into the future. It includes two tranches of foundational and modernisation work.

179. The 2023 risk documentation is comprehensive, includes all the elements of the 2019 framework and is updated in accordance with Commonwealth Government policy[16]. It now sits in the AEC's Risk Management System (ARMS), which is significantly better than what existed in 2019. The current AEC Risk Register and Strategic and Enterprise Risk Assessments, unlike the 2019 versions, explicitly recognise the personal safety of individuals as a risk consequence of a data breach.[17]

180. This gives confidence in the risk management framework at enterprise level but is something that the organisation can only benefit from if the project management and governance elevate the right risks.

181. To answer the question about how risks are identified, managed and elevated now, the Review considered the 2024 project management governance of Program Indigo. The conclusions were positive. Indigo has a continuity of governance right through from Technical Advisory level, and Agile Delivery Teams, a solution Management Team, Architecture Review Board, a Business Board, a Steering Committee, a single senior responsible officer and then

[16] AEC's Risk Management Framework is designed in accordance with requirements of S16 of the *Public Governance and Accountability Act 2013*, underpinned by ISO31000: 2018.

[17] Risk reference number 477, AEC 2024 Risk Register.

the Executive Leadership Team chaired by the Electoral Commissioner. The culture prioritises good governance and all levels focus on risk.

182. In March 2024 at AEC's invitation, the Digital Transformation Agency attended an Indigo Steering Committee (ISC) meeting at SES level. The post meeting written feedback is considered worthy of inclusion to illustrate the assessment of improved culture around project governance at AEC. The Acting General Manager for Investment Advice and Sourcing, Jamie Whitcombe advised the ISC Chair, First Assistant Commissioner Thomas Ryan.

> *From my wide engagement across digital projects in government, I can confidently say Indigo more than any other project has embraced the 'Culture and tone at the top' principle which sits at the centre of the Assurance Framework (for Digital and ICT Investments).*

183. Since 2023 the AEC has also had a high-level Transformation and Investment Committee (TIC), chaired at First Assistant Commissioner (SES Band 2) level. It includes among its 13 members the Assistant Commissioner responsible for the Indigo Delivery Branch.

184. This may appear to a reader outside government to be dense government bureaucracy, but unlike the governance for the SSP project and Register in 2019, it demonstrates no gaps in oversight, governance or responsibility for decisions.

So would AEC now actually identify a risk like the one in the Transparency Register project in 2019?

185. At project management level significant changes have been made. In 2019 the ICT project management documentation was, according to the current acting Assistant Commissioner for Enterprise Digital delivery, largely pro forma utilising the commonly used 'PRINCE2' methodology. It was fit for purpose as a methodology, but in the case of the Register it did not appear to the Review from available documentation and interviews, that the Steering Committee responsible for the Register was focused on the detail of the project. In turn, the Steering Committee did not appear to have been linked up with the higher-level strategic governance in the organisation.

186. Since then, the AEC introduced its current Project Management Framework in 2021. This provides project management guidance, doctrine and governance. The organisation has an Enterprise Project Management Office which answers to the TIC.

187. This looks good on paper, but the Review sought a practical understanding how risks would be visible and managed at working level. On 9 July 2024, officers responsible for 'Future State Candidate Management' (an important component of Indigo) kindly demonstrated their work to the Review.

188. The demonstration, which included concept screenshots of what the internal user will see and be using to enter data, was comprehensive. It gave assurance to the Review about how the proposed solution makes transparent its data sources and flags issues of concern. Of particular importance is the three-stage data verification approval process involving the initial digital data checks as a nomination is being submitted, a separate team member who must subsequently verify the work including data sources 'from scratch', and then an Executive Level delegate who must conduct final checks in order to approve a nomination.

189. This Review concluded that it would now be highly unlikely that a data link such as that made with the candidate nomination form postal address field in the Register in 2019, would go unremarked (or even allowed to remain in an early design of a system) at working level today.

This view is based on the Review observing the officers' awareness of the risks of moving data between systems; privacy concerns; and AEC silent elector responsibilities.

190. In a separate discussion, the Deputy Chair of the TIC, First Assistant Commissioner Rachael Spalding, told the review that the likelihood of identifying and managing a risk of the type that was undetected in 2019 is much higher as a result of the governance at all levels in place in relation to ICT projects in 2024. The Review concludes this confidence is not misplaced.

Finding 17: The AEC has implemented necessary changes to governance and project management of ICT projects in the AEC to minimise the risk of a future data breach similar to that which occurred with the Transparency Register.

191. Notwithstanding the above finding, this is something the AEC should test if it has not done so already.

Recommendation 8: That the AEC do a desktop exercise of its current ICT project governance framework using a contemporary scenario along the lines of the data breach to satisfy itself that it has mitigated the risk of a similar incident in the future to the extent possible.

Privacy Impact Assessment

192. The Review also considered the Transparency Register 2019 Privacy Impact Assessment (PIA) in the risk context. The PIA, prepared by Clayton Utz, was professionally prepared, but did not contemplate the inclusions on the Register that caused the data breach and data release issues. This is unsurprising. AEC itself had not made formal decisions on the inclusion of an address field filled with candidate nomination form data or identified the data release issue in any of its documentation. It cannot therefore expect to have briefed these issues to Clayton Utz. PIAs have no doubt matured since 2019, but if there is a lesson for the AEC to implement, it is the importance of the briefing it provides for the preparation of a PIA.

193. The Review makes no finding in this regard and notes the AEC's comfort with the robustness of the PIA process for the current Indigo project. As a sample, the Review examined the PIA Threshold Assessment for the Candidate Management Value Stream[18] element of Indigo. The increased level of detail and instruction about silent elector addresses was immediately evident.

Values

194. As the Electoral Commissioner himself remarked to the Review, the AEC prides itself on living its values. The Review was afforded an inside view of AEC in the National Office and the Melbourne State Office and through many interviews and conversations with staff. It experienced an organisation that is focussed on 'Electoral Integrity through Professionalism, Agility and Quality' at all levels.

195. This observation is tempered by the fact these AEC values existed at the time the Register was developed with the flaw that led to the data breach. One of the AEC professed characteristics of 'Agility', is maintaining "an awareness of the work of other business areas ...". The Review considered this worthy of consideration in the 2019 context.

[18] Candidate Management Value Stream Privacy Impact Threshold Assessment – Reference 070219

196. The AEC is a diverse and geographically disparate organisation. Multiple AEC officers have said that a relevant weakness they recall from the time the Register was developed, was that as committed as officers were at working level, their knowledge of what others did in the organisation was often not at a high level. This may well have contributed to the decision to use candidate nomination form postal addresses in entity banners on the Register. Those involved in developing the Register did not know enough about candidate nominations, and the work of those responsible for ELMS, to discern any risk.

197. This has been presented anecdotally to the Review and may not necessarily reflect the situation across AEC today, so no finding or recommendation is made. In fact, such innovations as a director-level operational committee (Director Operations and Readiness Group) that deliberately brings together the mid-level managers of the organisation indicate a current AEC focus on that aspect of 'Agility'. Nevertheless, the Review does think it is a point worth reflecting on in each branch of AEC. Understanding and valuing what other parts of the organisation do is a key ingredient of cohesion. It also helps ensure that risks are not left unaddressed in seams that can exist between committed work areas.

198. In conclusion, AEC SES and EL2 officers may wish to consider whether they are doing enough to encourage and enable their staff to understand and value what others in AEC do.

Are the lessons that must be implemented different for the data release issue than for the data breach?

199. Not all of the lessons that apply to the data breach apply to the data release. With the data release nothing was missed or done erroneously in a technical sense. And there was no project management shortcoming insofar as existing publicly available data from the Periodic Disclosure Tables was being imported into the Register. There was no new risk created – there was an existing risk that had escaped attention previously and continued to be missed during development of the Register.

200. In one respect this is similar to the data breach issue. The risk of there being silent elector addresses on returns that had to be published by law, was simply not surfaced in the organisation. The AEC Risk Register of the time did not contemplate the potential for Transparency requirements or the Register to cause silent addresses to be published.

201. The Review cannot conclude with the same confidence as for the data breach, that the 2024 risk, governance and project management arrangements would have stopped the data release in its tracks before a system went live. The vulnerability was not one born of the Register, but one the Register inherited.

202. The Review instead concludes that the risk management lesson to be implemented in respect of the data release to minimise the risk of a similar issue in the future relates to horizon scanning for where risks exist. The agency was highly focussed on security of silent electors on the electoral roll but did not focus on the risk of silent elector addresses being present elsewhere on a Register and not being identified as such.

203. While the AEC could offer the defence that it was only publishing what it was required to by law, rigorous horizon scanning internally as well as externally, may have increased the likelihood of the AEC recognising that release of silent elector addresses was a risk. This would have positioned it to discuss a legislative amendment with government and the Department of Finance, much earlier than 2024.

204. The AEC has clearly made major changes since 2019 and its risk documentation is of high quality. Its approach to Program Indigo gives confidence. But the length of time it took for the

data breach and data release issues to be identified means the AEC should ensure it is dynamic in identifying potential risks.

Finding 18: The AEC should review its Risk Register horizon scanning approach to ensure it is rigorous, regular and informed by changes in technology, and the internal and external security and privacy context.

205. The data release could have been recognised much earlier than 2024. Whether by good luck, or through more inquisitiveness by staff members as to why legislation would require publication of documents that could contain silent addresses, the matter may have been surfaced. That it was not, is a shortcoming, but not one of the type that led to the data breach.

206. Importantly, the way in which the AEC has responded since identifying the data release during the data breach investigation, indicates its willingness to own and address complex problems publicly. The review did not identify any specific additional lesson to implement in this regard.

Crisis and Incident Management

207. The lesson the AEC can implement with the most confidence out of the Register data breach and separate data release issue is that its crisis/incident management capability is strong. The Register problems represented an 'incident' not a 'crisis' (according to AEC's own doctrine), but the AEC response demonstrated sound fundamentals that will serve it well in crisis. The Review has one relevant recommendation (Recommendation 3) about including guidance on communication with other agencies in AEC's Incident and Crisis Management Framework. Even this is a preventative recommendation rather than one designed to remedy an actual shortcoming in what the AEC did.

208. Similarly, the Review also made a finding that the AEC should continue its communication with individuals affected by the data breach or data release as a priority. The Review is not suggesting there has been any shortcoming in this regard, but it should remain a priority.

Finding 19: The AEC should continue to exercise both its Crisis Management and Crisis Communications Framework regularly against a variety of contemporary scenarios. The Review acknowledges that the AEC will do this from a position of strength.

Acknowledgements

The Reviewer thanks all those in the AEC who have assisted the Review through interviews, provision of information and searches for documents. The level of cooperation reflects well on the AEC.

Thanks also to those officers from other agencies who gave up time to speak with the Review. Their contributions have been important.

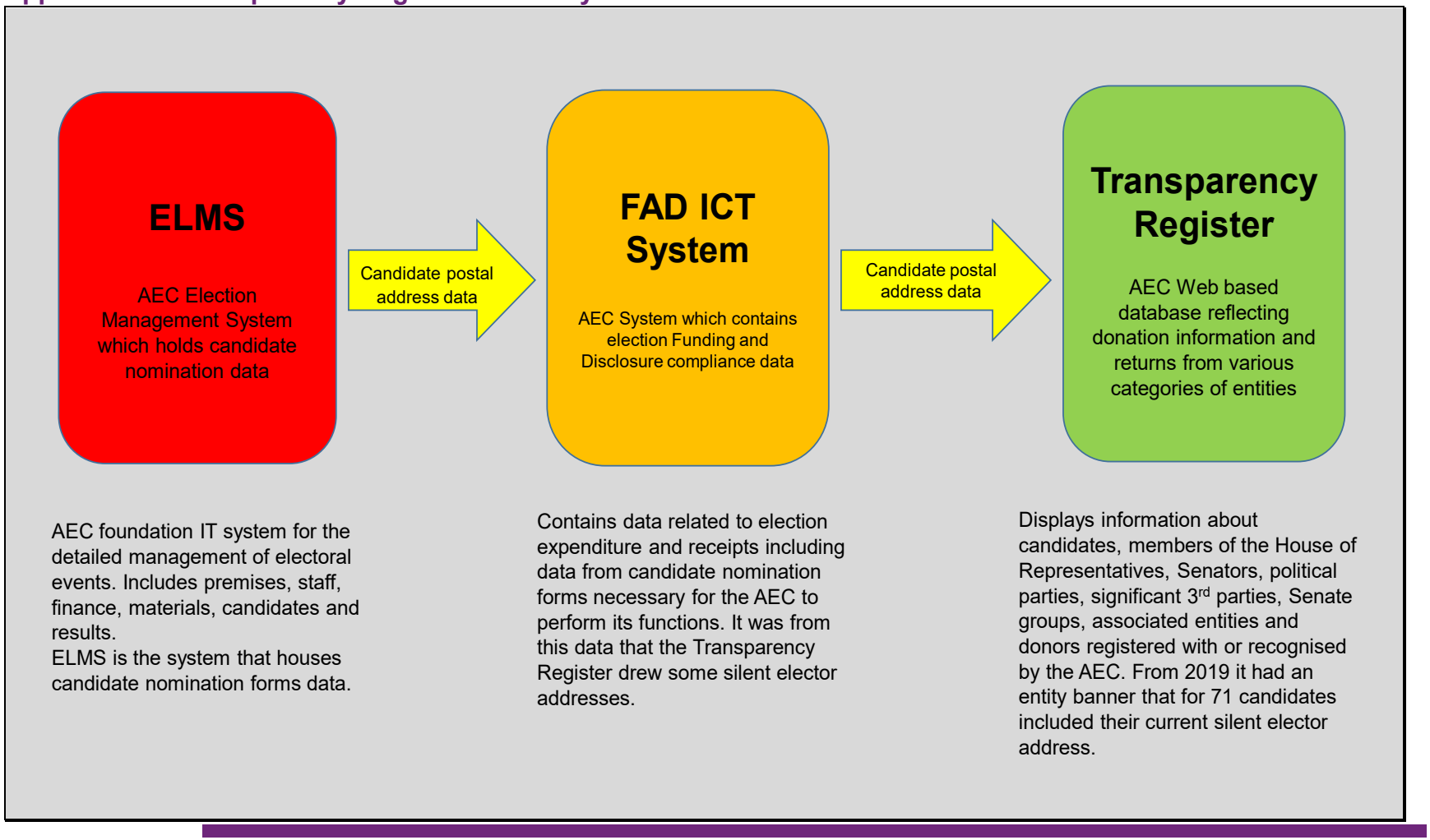
Special thanks go to Steve Kennedy, Rachel Dieckmann, Tessa Vincent, Rebecca Borys and Prisicilla Vosa for their wisdom, guidance and support throughout the Review. Without them it would not have been completed.

The recommendations and findings are those of the Reviewer.

Tony Sheehan
External Reviewer
31 July 2024

Appendices

Appendix A – Transparency Register related systems



Appendix B – List of meetings with the Review

Date	Attendees
4/06/2024	Privacy Officers, Director - Corporate Law
4/06/2024	Jo Reid (Assistant Commissioner, Disclosure, Party Registration and Redistribution Branch), Director - Disclosure and Compliance
7/06/2024	Director - Disclosure and Compliance, Assistant Director - Financial Disclosure, Assistant Director - Disclosure and Compliance
11/06/2024	Tania Wilson (First Assistant Commissioner, Chief Information Officer Division), Toby-Sly (Assistant Commissioner, Enterprise Digital Delivery Branch)
13/06/2024	Michael Lynch (First Assistant Commissioner, Electoral Integrity and Operations Group)
13/06/2024	Director - Disclosure and Compliance, Assistant Director - Financial Disclosure, Assistant Director - Disclosure and Compliance
14/06/2024	Jess Fraser (A/g Assistant Commissioner, Service Design and Foundations Branch), Director - Exercises and Rehearsals (led the Investigations Cell), Director - Roll Operations and Client Services
17/06/2024	Natasha Scandrett (Assistant Commissioner, Delivery and Support Branch), Director - Doctrine, Planning and Quality
17/06/2024	Cathie Kennedy (A/g Assistant Commissioner, Communication, Education and Engagement Branch)
19/06/2024	A/g Assistant Commissioner Stephen Fry (Australian Federal Police)
19/06/2024	Kath Gleeson - First Assistant Commissioner Service Delivery Group and National Elections Manager
20/06/2024	Karen Redhead (Assistant Commissioner, Indigo Product and Design Branch), Jess Fraser (A/g Assistant Commissioner, Service Design and Foundations Branch), Technical Service Design Lead, Business Analyst
20/06/2024	Matt Haigh (A/g Assistant Commissioner, Electoral Integrity and Media Branch)
20/06/2024	Jo Reid (Assistant Commissioner, Disclosure, Party Registration and Redistribution Branch)
21/06/2024	Kath Gleeson - First Assistant Commissioner, Service Delivery Group and National Elections Manager
25/06/2024	Natasha Scandrett (Assistant Commissioner, Delivery and Support Branch), Director - Doctrine, Planning and Quality
25/06/2024	Project Manager for SSP (2019-2020)
26/06/2024	Andrew Johnson (Chief Legal Officer)
27/06/2024	Rachael Spalding (First Assistant Commissioner, Enabling and Regulation Group)
27/06/2024	Director - IT Integration (Solution Architect - ICT Programs - Information, Communication and Technology Branch for SSP)
28/06/2024	Project Coordinator - IT Solutions, Toby Randall-Sly (Assistant Commissioner, Enterprise Digital Delivery Branch)
3/07/2024	Director - Media and Digital Engagement
3/07/2024	Project Coordinator - IT Solutions, Test Analyst, Assistant Director - Disclosure and Compliance
3/07/2024	Director - Exercises and Rehearsals (led the data breach Investigations Cell)
3/07/2024	Jo Reid (Assistant Commissioner, Disclosure, Party Registration and Redistribution Branch) and Assistant Director - Disclosure and Compliance
8/07/2024	Director - Indigo Product Management, Product Owner - Indigo Product Managment, Service Designer - User Experience
12/07/2024	Thomas Ryan - First Assistant Commissioner Enterprise Transformation Group and Senior Responsible Officer, Indigo Program.
17/07/2024	Jo Reid (Assistant Commissioner - Disclosure, Party Registration and Redistribution Branch) and Assistant Director - Disclosure and Compliance
18/07/2024	Director - Corporate Law
22/07/2024	Melanie Drayton (OAIC) - Deputy Commissioner and Andre Castaldi (OAIC) - Assistant Commissioner
25/07/2024	Director - Cyber Security and Assurance, Deputy IT Security Advisor, Cyber Security Governance Specialist.
Multiple	Tom Rogers (Electoral Commissioner)
Multiple	Jeff Pope (Deputy Electoral Commissioner)

Appendix C – Chronology

15 May 9.00am	Office of the Special Minister of State advised AEC that a parliamentarian had notified them that their residential address was displayed on the Transparency Register. The item was discussed by the Executive Leadership Team (ELT) where it was determined an Incident Management Team (IMT) should be stood up.
15 May noon	**IMT meeting #1**
15 May 1.45pm	Transparency Register taken offline.
15 May 4.00pm	**IMT meeting #2**
15 May 6.00pm	AEC attended and briefed an AFP-chaired Security Coordination Committee.
15 May 9.10pm	Impacted: Emails sent to two persons who were silent electors, advising current residential address was published. These were the first two AEC was aware of.
15 May 10.27pm	Email to AFP re details of the incident and actions taken.
15 May 10.31pm	Office of the Australian Information Commissioner (OAIC) informed via email.
15 May 11.11pm	Impacted: Emails sent to a further 20 persons who are silent electors advising current residential address was published.
16 May 10.30am	**IMT meeting #3**
16 May noon	Electoral Integrity Assurance Taskforce Board briefed.
16 May 4.00pm	**IMT meeting #4**
17 May 10.15am	**IMT meeting #5**
17 May 1.57pm	Impacted: Email to the 22* identified impacted persons sent, updating on investigation to date and advising access logs were being reviewed.
17 May 2.20pm	Media statement issued and published on AEC website.
17 May 4.20pm	Electoral Commissioner appeared on ABC Afternoon Briefing (Live TV).
17 May 7.14pm	Q&A published on the website with the media release.
17 May 8.23pm	Impacted: 54 further impacted persons notified that current address was published**
20 May 10.30am	**IMT meeting #6**
21 May 10.30am	**IMT meeting #7**
22 May 11.00am	**IMT meeting #8**
22 May 7.04pm	Impacted: Initial 22* impacted persons emailed outcome of investigation advising how many times their record had been viewed, and the dates.
23 May 10.00am	**IMT meeting #9**
24 May 10.30am	**IMT meeting #10**
24 May 2.30pm	Impacted: Electoral Commissioner emailed an apology with notifiable breach attached, to current silent electors whose address was known to be published in the data breach.
28 May 11.00am	**IMT meeting #11**
28 May 11.17am	OAIC advised AEC has sent formal notification of breach sent to impacted persons.

29 May	**IMT Meeting #12**
30 May	**IMT Meeting #13**
4 June	**IMT Meeting #14**
4 June	External Review of the data breach commences
11 June	**IMT Meeting #15**
18 June	**IMT Meeting #16**
22 July 3.56pm	AEC concludes assessment and formally informs OAIC of the notifiable data breach
25 July	AEC Transparency Register restored to AEC website without entity banner addresses or PDFs of original returns

* AEC's initial categorisation of number of persons at high risk in the data breach changed slightly over time, hence the difference between the numbers in the table above and the numbers in the body of the Review.

** AEC's assessment of the number of persons whose silent elector addresses were published changed slightly over time, hence the difference between the numbers contacted in the table above and the numbers explained in the Review. Only 17 of the 71 entity banners containing silent elector addresses were actually viewed. Those whose silent elector addresses were published but not viewed were assessed by AEC to be at lesser risk than the 17.

Appendix D – Documents Reviewed Registered

Document name	Document date
Forms	
Annual Return – Individual Donor Contact Information form	2023-24
Annual Return – Third Party Contact Information form	2023-24
Annual Return – Senator Contact Information form	2023-24
Annual Return – Member of the House of Representatives Contact Information form	2023-24
Associated Entity Disclosure Return form – Financial Year	2023-24
Candidate Return form - For 2022 Federal election	21 May 2022
Election Donor Return form - For 2022 Federal election	21 May 2022
Political Party Disclosure Return form	2023-24
Significant Third-Party Disclosure Return form	2023-24
Risk	
2019 Risk Appetite Statement	2019
2019 Risk Management Policy	March 2019
2019 Risk Matrix and Escalation Table	2019
2019 Risk Register	2019
2019 Strategic Enterprise and Risk Statement	July 2019
2023 Risk Management Policy	August 2023
2023 Enterprise Risk Reporting Framework	August 2023
2023 Risk Appetite Statement	August 2023
2023 Risk Management Guidelines	August 2023
2023 Risk Matrix and Consequence Table	August 2023
AEC Risk Register	12 July 2024
AEC Strategic and Enterprise Risk Register	12 July 2024
Executive Leadership Team (ELT) Meeting – Agenda Paper – Table 1 AEC Strategic and Enterprise Risks Statement - ELT endorsed	1 July 2019
Privacy	
AEC Privacy Management Plan	2019-2020
AEC Privacy Management Plan	2023-2024
Candidate Management Value Stream – Privacy Impact Threshold Assessment	May 2024
AEC Self-Service Platform Releases 1-3 Privacy Impact Assessment	October 2019
Transparency Register	
Executive Leadership Team (ELT) Meeting - Transparency Register Options	24 June 2024

Document name	Document date
Executive Leadership Team (ELT) Meeting - Transparency Register – Privacy Breach Notification for AEC Website	24 June 2024
Meeting Minutes - Incident Management Team (IMT): Transparency Register (various meetings)	15 May – 18 June
Email from First Assistant Commissioner, Enabling and Regulation Group to AllStaff-AEC@aec.gov.au – Subject: ALL STAFF MESSAGE: AEC Transparency Register Temporarily Offline	16 May 2024
Email from Assistant Commissioner, Disclosure, Party Registration and Redistribution Branch to persons at high risk affected by the Data Breach (x22)	15 May 2024
Email from Deputy Electoral Commissioner to SES – Subject: Information regarding the Transparency Register	15 May 2024
AEC Question and Answer document - AEC Transparency Register	3 June 2024
Media Release	
AEC Media Release - AEC Statement: Transparency Register	17 May 2024
ABC Radio – News headline example with Evan Ekin-Smyth	17 May 2024
ABC Afternoon Briefings interview – Electoral Commissioner	17 May 2024
Frameworks	
AEC Project Management Framework July 2021 (And Complexity Assessment Tool (CAT) Guidance)	July 2021
AEC External incident and crisis communication framework	5 March 2024
AEC Corporate Plan	2023-24
AEC Corporate Plan	2019-20
AEC Annual Report	2023-24
AEC Annual Report	2018-19
Committee papers	
Disclosure, Assurance an Engagement Branch Clearance Record – SSP Program Project Management Plan V1.1	7 Nov 2024
Self Service Platform Project - Production Readiness Checklist – Reporting period 4-17 Oct 2019 - Status date 19 Oct 2019	19 Oct 2019
Self Service Platform Project - Production Readiness Checklist – Reporting period 15 Nov – 9 Dec 2019 - Status date 9 Dec 2019	9 Dec 2019
Self Service Platform Project - Project Management Plan V1.5	17 May 2019
Self Service Platform CEF Daily Stand-up Task Tracker	20 Sept 2019
Self Service Platform Project Weekly Highlight Report	16 Oct 2019
Self Service Platform Project Closure Report V0.6	June 2023
Regulations	

Document name	Document date
Electoral and Referendum Amendment (Eligibility) Regulations 2018 - F2018L00669	29 May 2018
Explanatory Statement - Electoral and Referendum Amendment (Eligibility) Regulations 2018 - Issued by Authority of the Minister for Finance - Commonwealth Electoral Act 1918 - F2018L00669ES	29 May 2018
Investment, Change and People Strategy Committee – Agenda Paper item 4 - Project Management Office Redesign and Implementation	18 Feb 2021
Investment, Change and People Strategy Committee – Agenda paper item 6 - Project Management Office – Current State Analysis & Initial Findings	18 Feb 2021
Project Closure Report – Project Closure Report - Security Service Edge (SSE) Proof of Value (PoV) V1.2	June 2024
Project Management Plan – Self Service Platform V3.4a	August 2021
Other	
Self Service Platform (SSP) Solution Architecture Definition V12	10 Feb 2020
APSC National Survey in Trust and Satisfaction in Australian Democracy	2023
Trust in Australian public services 2023 Annual Report	2023
Proposed Website – Menu structure and dev content (for purpose of release 1 of Self-Service Platform)	2019
Communication response plan – cyber security breach	30 April 2024

*For reasons of length the Documents Reviewed Register does not contain records of all documents received or viewed