nesa

NESA'S Response to the

Disability Employment Services

The new specialist disability employment program: Draft Deed

September 2024

General Comment

NESA appreciates the opportunity to provide feedback on the Draft Deed for the new specialist disability employment program and welcomes the opportunity to discuss with the Department any of the issues raised below in greater detail.

NESA strongly opposes any requirements under the Deed that will increase the administrative burden upon providers.

It is also critical that this feedback is read in conjunction with NESA's feedback provided on 30 August 2024 in response to the Exposure Draft of the Request for Tender, including NESA's feedback in relation to:

- Staff qualifications
- Payments model
- Generalist and Specialists
- Intensive and Flexible Services
- Appointments and Contacts
- Ongoing Support
- Transition Arrangements
- Market Structure.

Clause	FEEDBACK	
11.3	"The provider must ensure that its Site(s) are established and fully operational in the suburb(s) specified in item 0 or 0 of schedule 1 – Deed details by no later than 1 July 2025, unless a different start date for the Site is specified in item 00 of Schedule 1 – Deed details.	**Concerns:** Sufficient timing must be allowed between notification of the outcome of the tender and commencement. Unless site locations are known well in advance of 1 July 2025 it will be difficult for a provider to secure a suitable building lease, fit-out, recruit and train staff, and be operational. There needs to be sufficient lead time to allow establishment of services. For example, NBN connectivity can take up to 120 days to provision services; and it can take between 2- 3 months to recruit and train new staff so they are ready for operation on Day 1. These could trigger a breach under clause 11.4. **Feedback:** Tender outcome notification must be no later than 120 days prior to commencement of the contract to enable compliance with the Deed and provide sufficient time for establishment of the service.
39.3	The Department may require that specific data must only be stored on the Department's IT Systems, and the Provider must comply, and must ensure that any Subcontractors, auditors and Third-Party IT Vendors, comply with any such requirements.	**Concerns:** The requirement for specific data to be stored only on the Department's IT systems raises questions regarding the types of data that fall under this restriction. Providers are concerned about potential operational impacts, especially if there is no clear guidance on what data is prohibited from being stored outside the Department's systems. This could complicate data management processes, such as importing data into systems like JRL or an internal reporting database. There are also known functionalities missing from the current DEWR system to which the new program is being transferred (eg., the ability to upload resumes).

		Feedback: Successful tenderers need clarification from the Department as to whether such requirements have been implemented previously; including a comprehensive listing of data that is not permitted to be stored outside of the Department's systems. This would ensure that a provider and its subcontractors can manage data effectively while remaining in full compliance with the Deed.
40.9	If a Provider IT System is modified, the Provider must take all steps necessary to obtain RFFR reaccreditation for that Provider IT System in accordance with the requirements and timeframes set out in the ESAF.	**Concerns:** The ESAF only lists recertification requirements based on regular scheduled recertification. It does not indicate what changes would require recertification, nor the requirements for recertification should something change. **Feedback:** The Department should clarify what changes would require recertification and what the recertification process would be in these circumstances. For example, if a category 1 provider replaces infrastructure devices but implements all previously accredited SoA controls - is an external audit still required to validate and provide assurance?
40.17	The Provider must comply, and must ensure that its Personnel (including Subcontractors and their Personnel) and Third-Party IT Vendors comply, with: (a) all relevant requirements specified in: (i) Security Policies of the Department and DEWR; and (ii) the Protective Security Policy Framework.	**Concerns:** The Protective Security Policy Framework (PSPF) is primarily designed for Australian Government agencies and includes many requirements that may not be suitable or practical for providers outside of government. The PSPF encompasses 16 policies that impose significant obligations, such as the need for an "accountable authority" who reports directly to government ministers and adherence to government-specific Security Classifications like Official:

Sensitive. The security requirements as stated under the draft Deed will necessitate substantial personnel (vetting/screening), ICT and cyber security enhancements, including labelling and protective marking systems, which are typically expensive and required in the private sector.

Feedback:
It is NESA's understanding that the ESAF was created so that compliance with PSPF itself was not required. In the case of category 1 providers, this was the ISO 27001 certification, intended to be a practical, implementable, and measurable way to address many of the management system requirements from PSPF while not requiring the internal government-specific bureaucratic components). At the same time, it included the benefits from the Information Security Manual (ISM) and Essential Eight cumulatively for the Right-Fit-For-Risk approach.

Feedback:
The Department should remove this requirement, or amend this clause to provide an exemption for, or tailoring to, the context of individual providers given the unique circumstances of non-government entities and reflect the original purpose of the ESAF and RFFR when mandating compliance with the PSPF. Security requirements should also align more closely with the existing operational frameworks of providers. This would ensure unnecessary complexities and costs are avoided, while maintaining appropriate security controls that are practical and able to be implemented outside of Government.

40.19	If the ESAF requires that any of the Provider Personnel, including Subcontractor Personnel, must obtain security clearances for the purposes of accreditation or reaccreditation or the Department otherwise Notifies the Provider that particular Personnel must hold a particular level of Commonwealth security clearance: (a) the Provider must ensure that the relevant Personnel obtain, and maintain, the required security clearances, and bear any costs associated with doing so; and (b) the Department will sponsor such clearances as required by the ESAF	**Concerns:** On 23 August 2023, The Australian Government changed Official: Sensitive from being a Dissemination Limiting Marker to a Security Classification with the caveat that a Baseline Security clearance was not required to access this type of information given 'employment screening for agency personnel remains sufficient'. However, it is not clear whether this policy will change under this program. There is significant concern in the sector that should the PSPF change, and a requirement for all provider's staff to have Baseline Security clearances be introduced, a provider's ability to attract and retain personnel (particularly the requirement to be an Australian citizen) will be critically impacted. As it currently stands, the requirement for personnel to obtain security clearances (see PSPF Policy 12), includes extensive pre-employment screening obligations, such as identity verification through the Document Verification Service, confirmation of eligibility to work in Australia, and assurance of suitability to access Australian Government resources. Additional security requirements will impose significant additional costs on the Provider (not funded for under the contract), particularly concerning the use of services like the Document Verification Service and credit history checks. **Feedback:** The Department should clarify exactly what the obligations are for employee screening in order to access Departmental Systems and/or customer data (ie. Official: Sensitive) information. The Department should also clarify whether any additional funding or assistance will be made available to cover the costs associated with

		additional screening obligations. Without such support, the financial burden on Providers will be considerable, impacting their ability to deliver services effectively and efficiently.
40.20	The Provider is responsible for all costs associated with obtaining security clearances.	**Concerns:** The obligation for the Provider to bear all costs related to security clearances could have significant financial implications, especially if the requirements extend to obtaining Baseline Security clearances for accessing Official: Sensitive information. The cost of these clearances, including the $884 per person fee and the requirement for Australian citizenship, may place considerable strain on a Provider's resources. **Feedback:** The funding model should be adjusted to reflect the significant costs associated with obtaining security clearances. The impact will be significant upon all providers, but particularly small providers if the costs are not reflected in the funding received. An alternative option is for the Department to consider implementing a cost-sharing arrangement or providing financial support to mitigate the impact of these security clearance requirements. This would ensure that Providers can meet the necessary clearance obligations without compromising their operational or financial stability.
40.21	The Provider must not permit any of its Personnel to have any access to Security Classified Information unless: (a) the relevant person has been cleared to the appropriate security level; and b) the relevant person has complied with all directions by the Department relating to access to, and use of, the Security Classified Information.	**Concerns:** The concerns with clause 40.21 align with concerns/feedback provided in relation to clause 40.19. Providers do not currently require personnel to obtain security clearances, as existing processes involve primarily police checks.

		However, ICT administrators are Australian citizens. The introduction of mandatory security clearances could significantly restrict a Provider's ability to assign tasks effectively, potentially leading to delays in project timelines and necessitating additional resources to manage the clearance process. **Feedback:** It is recommended that the Department consider implementing a more flexible approach such as allowing personnel to access lower levels of classified information such as under temporary access provisions. This would partly alleviate the burden of requiring full security clearances.
50	The Department reserves the right to conduct assurance activities and audits to ensure compliance with the Deed.	**Concerns:** Providers currently manage audits through a combination of internal assessments against ISO 27001 and external audits under the Department's RFFR scheme. It should be noted that any additional audits proposed under the Deed will require the allocation of significant resources for preparation and response, potentially diverting focus from ongoing service delivery. It is also noted there is a discrepancy in definitions of data-breach between the DEED and the DEWR RFFR Scheme as interpreted by JASANZ and certifying bodies. It currently exists in the RFFR scheme, that *any* data breach (no matter how minor) must trigger a short-notice audit (costing days of effort and attracting thousands of dollars of audit fees) rather than only an "eligible data breach" as per the DEED as per the OAIC / Privacy Act, Notifiable Data Breach Scheme. **Feedback:** The Department should clarify for ESAF/RFFR purposes relating to data-breaches that only Eligible Data Breaches as per the Notifiable Data Breach Scheme will require short-notice audits.

		The Department should also state the expected frequency and specific focus areas of these audits to enable prospective providers to allocate resources efficiently. This would enable a provider to maintain a balance between compliance and the continuation of high-quality service delivery.
52	The Provider must at all reasonable times give or arrange for any Department Employee who is assessing the Provider's compliance with its obligations in the Deed.	**Concerns:** The Deed does not sufficiently protect the confidential (non-Departmental information) held by providers. The broad access rights granted to the Department under the Deed also raise significant cyber security concerns, particularly regarding the potential exposure of sensitive systems and data to systems containing non-Department-related data and commercial in confidence information. **Feedback:** The Department should negotiate with individual providers the specific terms regarding Departmental access to its premises and IT systems. This should include limitations being place on the Department so that it can access Departmental data **only** (and systems it resides on), non-sensitive areas, and place an obligation on the Department to ensure that strict oversight is maintained during inspections to prevent inadvertent data breaches by the Department or their representatives.
53	Providers must indemnify the Department against any claims arising from their breach of the Deed or negligence in delivering services.	**Feedback:** The Deed (being an agreement between two parties), should also enable providers to recoup losses/damages from the Department due to a fault by action or inaction of the Department and/or its personnel.

63	Establishes a process for resolving disputes between the Provider and the Department.	**Concerns:** The dispute resolution process as outlined in the Deed could delay the resolution of urgent issues, particularly those impacting service delivery. **Feedback**: It is requested that the Department clarify the timelines for each stage of the dispute resolution process to ensure that critical issues can be addressed swiftly. This would help minimise disruptions to service delivery during resolution of a dispute.
93	Providers are required to notify the Department of any significant events that could impact service delivery.	**Concerns:** Providers currently have a clear process for reporting data breaches to the Department. However, the broader requirement in the Deed to report significant events could impose additional administrative burdens, especially if the definition of "significant events" is not clearly defined. **Feedback:** The Department should clarify what qualifies as a "significant event" and provide a streamlined reporting process to reduce administrative overhead while ensuring the Department is kept informed of critical issues in a timely manner.
54.1eiii	in respect of: loss of, damage to, or loss of use of any real, personal or intangible property (including property of the Department in the care, custody or control of the Provider, and including the Department's IT Systems)	**Comment** Clause 54 requires providers to have and maintain insurance. However, the clause contains a requirement for insurance to cover 'loss of use of any …intangible property' which is outside the scope of normal liability insurance policies, risking providers being in breach of the Deed due to being unable to obtain the specified coverage.

		Feedback It is strongly recommended that the Deed omit requirements to cover damage to, or loss of use of intangible property as this extends beyond the scope of general liability insurance policies.
54.4 (B)	a waiver of subrogation clause, whereby the insurer agrees to waive all rights of subrogation or action that it may have or acquire against any or all of the entities insured (at least to the extent that they are insured under the policy).	**Feedback** It is recommended that clause 54.5(b) be omitted from the Deed, given this is not appropriate for professional indemnity and cyber insurance policies. Waiver of subrogation clauses are typically relevant to liability insurance policies alone.
53.1	Provider must indemnify Dept and its personnel (officers, employees, volunteers, and professional advisers) for any loss, damage, expenses arising from: "any breach" of deed; third party IP infringement and other IP-related loss; information provided by Provider and published by Dept; and any act/omission "if there was fault of the part of the **person** whose conduct gave rise to that Loss".	**Feedback** It is recommended that clarification is provided on if that "person" (see bold) should be changed to (or is intended to refer to) "Personnel of the Provider".
41	IP Ownership	**Comment** The definition of Deed Material para (b) includes material created for the purposes of performing the Deed. This could be existing IP or Third-Party IP to also constitute Deed Material. **Feedback** It is recommended this is fixed by including an express carve out of Existing IP and Third-Party IP from the definition of Deed Material.