SCHEDULE 17 - The Provision of ADF Records and Information Services of Serving and Former Members under MoU Cooperative Delivery of Care and Support to Eligible Persons

Cover Sheet:

1. Description of Services/Agreement:

1.1. This Schedule outlines the commitments of the Department of Defence (Defence) and the Department of Veterans' Affairs (DVA) for the provision of ADF records and information services between DVA and Defence. It outlines the principles for a coordinated, single point of contact approach, commonly referred to as the Single Access Mechanism (SAM) for how DVA requests and receives information from Defence relating to serving and former Australian Defence Force (ADF) members (including Reservists) and their dependants.

1.2. Through the SAM, DVA and Defence agree to provide one another with timely access to information required by each Department to conduct its business effectively.

1.3. This Agreement commences on the day signed between both Defence and DVA (contained in the Signature Page to this Schedule), and concludes 5 years after date of signature.

1.4. DVA and Defence agree to consult on a new Agreement to replace this current Agreement commencing no later than six months before the expiration of the current Agreement. If a new Agreement has not been finalised before its expiration, the current Agreement will remain in force until a new Agreement is finalised.

2. Key Points of Contact:

	Defence	**DVA**
Position	*Director General* *Defence Community Organisation*	*Assistant Secretary* *Clients' Benefits Processing Team 2*
Postal Address	PO Box 7921 Canberra BC ACT 2610	GPO Box 9998 Brisbane QLD 4001
Telephone	s47E(d)	s47F
E-mail	s47E(d)	s47F

1. The Provision of ADF Records and Information Services of Serving and Former Members

1.1. This Schedule outlines the commitments of the Department of Defence (Defence) and the Department of Veterans' Affairs (DVA) for the provision of ADF records and information services between DVA and Defence.

1.2. In accordance with Clause 7.2 of the Memorandum of Understanding between Defence and DVA, and in conjunction with the *Guidelines for the Single Access Mechanism* (SAM Guidelines), this Schedule describes the basic responsibilities and sets out the necessary principles for how Defence and DVA information will be managed through the SAM function.

1.3. This Schedule takes effect on the date signed by both Defence and DVA representatives on the signature page. Once signed, this Schedule incorporates the provisions of ADF Records and Information Services of Serving and Former Members and forms part of the MoU between Defence and DVA for the Cooperative Delivery of Care and Support to Eligible Persons.

1.4. The *Privacy Act 1988* (the Privacy Act), the *Freedom of Information Act 1982* (the FOI Act) and the *Archives Act 1983* (the Archives Act) underpin the way in which Defence and DVA request, collect, store, use, and release personal information obtained through the SAM.

2. Description of Services/Agreement:

2.1. DVA requires specific information contained within Defence records and systems to assess the basis of a claimant's entitlements when they lodge a claim with DVA. Through the SAM, and in reference to the Governing Principles of the MOU, DVA and Defence agree to provide one another with access to information required by each Department to conduct its business effectively. This will be achieved by:

- constantly improving the timeliness and transparency in records and information management;
- supporting self-sufficiency by providing DVA access to a range of Defence ICT systems to facilitate direct access to records and information (where possible):
    - Schedule 20 to the MOU details the scope, processes, protocols, and obligations of both departments that underpin access to Defence ICT;
    - Under the auspices of Schedule 20 to the MOU, the provision of access to Defence ICT systems allows DVA to be more self-sufficient, and in doing so, reduces the time taken to source required information to facilitate timely determination of claims; and
- consistently striving for higher service delivery outcomes through open dialogue, process review, and improvement initiatives.

2.2. This Schedule does not include provision of the following:

- Records regarding Australian Defence Organisation involvement in operations which are coordinated by United Nations or NATO where those records are not created by Defence.
- Service on submarines in relation to special operations 1978-1992. Due to security restrictions, it is not possible to verify the locations of submarine operations, the timing of submarine operations, which submarine the operation was conducted on and what operations the submarines were tasked to conduct. s22 provides further information for DVA claims assessors.

3. Protected Identities Personnel Records:

3.1. Protected Identities personnel records will be sensitised by Defence prior to provision to DVA. This is to preserve the Protected Identity status of other members that may be identified in these records. Examples of this are unit level administrative documentation and course reports.

Part A: Single Access Mechanism (SAM) Services

1. The primary objective of the SAM (the Mechanism) is to provide DVA with specific Defence records and information in response to official requests made under the *Veterans' Entitlements Act 1986* (VEA), the *Military Rehabilitation and Compensation Act 2004* (MRCA), the *Safety, Rehabilitation and Compensation (Defence-related Claims) Act 1988* (DRCA), the *Defence Service Homes Act 1918*, and the *Australian Participants in British Nuclear Tests and British Commonwealth Occupation Force (Treatment) Act 2006.*
2. Defence and DVA will each provide a SAM coordination team that will be the single point of contact between both departments. The SAM teams will action and monitor requests from DVA claims assessors for Defence records and information for the purpose of investigating claims for liability and compensation.
3. Before sending a request to Defence SAM, the DVA SAM will ensure the request is adequately quality assured and contains actionable and verifiable information required by Defence and that requests are made under the authority of an appropriate Act. Only requests sent by the DVA SAM team will be recognised by the Defence SAM team as being authorised by DVA.
4. On receiving requests from DVA SAM, the Defence SAM team will check the request contains sufficient details for it to be actioned. Requests that contain sufficient details will be distributed to the relevant Defence area and track the progress of each request in accordance with agreed timeliness standards. If the request from DVA is too broad in scope, too speculative, or contains errors that could lead to a wrong or inconclusive outcome, Defence SAM may return the request to DVA SAM as an Incorrect DVA Request (IDR), with explanation, for clarification, adjustment and resubmittal. Replies to DVA will only be sent via the Defence SAM team.
5. Upon access to, or receipt of, information/records from the relevant Defence area or ICT system, both Defence and DVA SAM teams will provide a level of quality assurance: to ensure the information/records address the original request, and to mitigate the risk of privacy breaches before provision to the DVA claims assessors.
6. The operational parameters, processes, and procedures for the SAM function will be documented in the *Guidelines for the Single Access Mechanism* (SAM Guidelines). Defence and DVA will collaborate on regular reviews and be jointly responsible for ensuring the currency and validity of the information contained in the SAM Guidelines. These guidelines inform DVA Assessors and Delegates on developing actionable requests for information.

Part B: Obligations and Work to be Performed

7. The obligations and work to be performed by Defence and DVA stakeholders are outlined in the SAM Guidelines. At the request of the Secondary Points of Contact, the Authorised Points of Contact may consider and endorse variations to the SAM Guidelines and also determine effective commencement dates for the changes.

Part C: Facilities and Accommodation Requirements

8. Not applicable

Part D: Funding Schedule

9. Not applicable

Part E: Personnel Required

10. Not applicable

Part F: Monitoring, Reporting and Evaluation

11. Reporting on Defence and DVA performance and business outcomes of the SAM function is outlined under Schedule 19 to the MOU.

Part G: Performance Measures and Standards

12. Defence and DVA will strive to attain a year to date average that 95% of all requests are completed on time. The Performance Measures and Standards for Defence SAM will be defined in their operating procedures and those for DVA SAM will be defined in their SAM Guidelines. At the request of the Authorised Points of Contact, the Defence Links Steering Committee (DLSC) may consider and endorse variations to the SAM Guidelines and also determine effective commencement dates.

13. The timeframes allocated for the provision of requested information, by Defence to DVA, is outlined below:

Table 1: Priority of Requests:

Priority	Within 12 Months of Separation or Currently Serving	Between 1 to 3 years from Separation	3+ years of Separation
Urgent (General)	5 business days **(UG - Category 1)**	10 business days **(UG - Category 2)**	15 business days **UG - Category 3**
Urgent (Complex)	20 business days **UC - Category 1**	20 business days **UC - Category 2**	30 business days **UC - Category 3**
Medium	15 business days **Category 1**	20 business days **Category 2**	25 business days **Category 3**
Routine	25 business days **Category 1**	30 business days **Category 2**	35 business days **Category 3**

Table 2: Categories for Priority Requests

Urgent (General)	Urgent (Complex)	Medium
Financial hardship This priority includes: - Clients who are transitioning - Clients who have recently transitioned - Any individual without an income - If the financial information is detrimental to the well-being of the individual - A reservist who has pending surgery and will be without civilian income	**Cases with the VRB or AAT** This priority includes: - Military Research requests - Any client who has an appeal with the AAT	**Death Payments** This priority covers: - war widows and/or dependants who are already receiving some form of payment and therefore has less financial impact. **All Incapacity Payment claims** (where no financial hardship has been identified)
High Profile - A client who is identified as high profile by DVA Executive, Minister or Ombudsman - Clients who are involved in incidents that have received public attention - When a client is deemed by either DVA or Defence to be a reputational risk.	**Member is over 90 years of age** - Where a client who has lodged a claim is 90 years of age or older.	
Death or Imminent death - Where a request for information is for an individual who has a terminal illness or has died.		
Defence Priority - All claims that have been highlighted by Defence as being a priority		
At Risk – Mental health or Serious injury - when information is requested for an individual who has presented to DVA with a mental health condition - when a delegate deems a client is at risk - Homelessness or at risk of homelessness		

Part H: Special Provisions

14. Defence and DVA acknowledge that from time to time exceptional circumstances may require specific situations to be handled differently from the standard SAM process. In these situations, and at the specific request of the relevant Director, *URGENT – CRITICAL* requests may be initiated that require an immediate response. These requests may relate to:

- Clients who are identified as suicidal and unstable, or at risk of severe self-harm, or harm to others;
- Severe financial hardship on the grounds of loss of income due to medical transition and/or cessation of employment due to accepted conditions;
- Homelessness and/or severe welfare concerns; and
- Politically sensitive/high profile cases

15. DVA acknowledges that physical Defence records are the property of Defence and is the major user of its medical records. Defence and DVA are accountable for the storage and management of these records whilst in the possession of each Agency. When requested, DVA agrees to return original medical records to Defence in a timely manner.

16. It is noted that historically Defence and DVA agree the following medical records are in the custody of DVA:

- Navy - Served and separated prior to 1948
- Army - Served and separated prior to 1947
- Air Force - Served and separated prior to 1952

Part I: Authorised Points of Contact and Addresses for Notices

	Defence	**DVA**
Position	*Director General* *Defence Community Organisation*	*Assistant Secretary* *Clients' Benefits Processing Team 2*
Postal Address	PO Box 7921 Canberra BC ACT 2610	GPO Box 9998 Brisbane QLD 4001
Telephone	s47E(d)	s47F
Fax		
E-mail	s47E(d)	s47F

Secondary Points of Contact

	Defence	**DVA**
Position	*Director* *Community Support & Information Services*	*Director* *Performance, SAM, and Accounts*
Postal Address	PO Box 7921 Canberra BC ACT 2610	GPO Box 9998 Brisbane QLD 4001
Telephone	s47E(d)	s47F
Fax		
E-mail	s47E(d)	s47F

THE SIGNATURES PAGE

Signed for and on behalf of the Department of Defence	
by: s47E(d)	Director General, Defence Community Organisation
Signature and date: s22	7/11/19
Witnessed by: s47E(d)	
Signature and date: s22	7/11/19

Signed for and on behalf of the Department of Veterans' Affairs, the Repatriation Commission and the Military Rehabilitation and Compensation Commission	
by: s47F	Assistant Secretary, Clients' Benefits Processing Team 2
Signature and date: s22	12/12/19.
Witnessed by: s47F	
Signature and date: s22	11/12/19

Definitions

Australian Defence Force (ADF)	Means current and serving members of the Royal Australian Navy, Australian Regular Army, and Royal Australian Air Force (including, their Reserve components).
Attachment	Means a document attached or referred to expressly by a clause as describing a relevant aspect of this SLA.
Commonwealth	Means the Commonwealth of Australia.
Defence Records	Means any record created by Defence that requires access by DVA in order to determine claims for entitlement.
Military Rehabilitation and Compensation Commission (MRCC)	Means the body corporate enacted under the Military Rehabilitation and Compensation Act 2004 or any other government agency that carries out functions equivalent to the Military Rehabilitation and Compensation Commission.
Party	Means, as applicable, Defence, DVA and their respective personnel.
Repatriation Commission	Means the body corporate continued in existence under the Veterans' Entitlements Act 1986 or any other government agency that carries out functions equivalent to the Repatriation Commission.
Schedule	Means an agreement under the Defence and the Department of Veterans' Affairs Memorandum of Understanding between Defence and the Department of Veterans' Affairs for the supply of a service at an agreed standard. This Schedule includes the clauses, Annexes and Attachments, but does not include the title page, table of contents or heading; however, these may help clarify any inconsistencies.
foreseen event	Means any event or combination of events which is beyond the control of a party (the 'affected party') and which causes a default or delay in the performance by the affected party of its obligations under this SLA and where such an event could not have been prevented or overcome by that party exercising a standard of care and diligence consistent with that of a prudent and competent person operating within the relevant industry/profession, and which may include, for example: • elements of nature such as fire, flood, or earthquake; • acts of war, terrorism; or • an act or omission by a third party causing major prolonged disruption of infrastructure, telecommunications or electricity services where the impact is significant and where such act or omission by the third party is beyond the control or influence of Defence or DVA.

Date of Schedule: **5 July 2022**

SCHEDULE 20

ARRANGEMENTS FOR ACCESS TO, OR THE DISCLOSURE OF, CERTAIN PERSONAL INFORMATION

Cover Sheet

Description of Services/Agreement:

This Schedule sets out the arrangements under which Defence and DVA provide access to, or disclose, certain Personal Information held digitally in specified Departmental information systems.

The Schedule details the scope of, and processes and protocols that underpin, such access, or disclosure as well as setting out the obligations placed on both Departments in respect of the associated administration.

The Schedule also establishes the compliance arrangements associated with such access and details the relevant points of contact and escalation processes to be used in the event of a disruption to the agreed access arrangements.

Key Points of Contact/Authorised Officers:

	Defence	**DVA**
Position	Director General Veterans' Support	Assistant Secretary Claims Assessment and Management
Postal Address	s47E(d) Brindabella Park Offices PO Box 7927 Canberra BC ACT 2610	GPO Box 9998 Brisbane QLD 4001
Telephone	s47E(d)	s47F
E-mail	s47E(d) @defence.gov.au	s47F @dva.go.au

Expiry Date: 5 July 2027

Date of Schedule: 5 July 2022

ARRANGEMENTS FOR ACCESS TO, OR THE DISCLOSURE OF, CERTAIN PERSONAL INFORMATION

This Schedule sets out the arrangements under which the Department of Defence (Defence) and Department of Veterans' Affairs (DVA) provide access to, or disclosure of, certain Personal Information held digitally in specified Departmental information systems.

This Schedule takes effect once signed by both Parties and incorporates the provisions, of the Memorandum of Understanding (MoU) between Defence and DVA for the Cooperative Delivery of Care and Support.

Schedule Number: 20

Title: Arrangements For Access To, Or The Disclosure Of, Certain Personal Information

Description of Services/Agreement:

Defence and DVA are committed to sharing relevant information to:

a. ensure that assessment and determination of claims occurs in a timely manner and as close as possible to the time the injury, and

b. enable the delivery of the appropriate care and support.

Providing efficient and timely access to, or the disclosure of, certain Personal Information held digitally in specified Departmental information systems supports this commitment. Such access, or disclosure, removes bottlenecks in information flows, reduces the burden on both Departments in sourcing information relevant to considerations, improves the timeliness of determinations and facilitates the efficient dissemination of claims-related documentation. More importantly, more efficient and timely access, or disclosure, directly benefits current and former members and their families.

The Schedule details the scope of, and processes and protocols that underpin, such access or disclosure as well as setting out the obligations placed on both Departments in respect of the associated administration.

Access to personal information held within either Department will be by either individual direct access or through established system to system integration. Where specific requirements associated with any data exchange need to be detailed and agreed, as is the case in system to system integration, a Data Management Agreement (DMA) will be required. Once signed by both parties, DMAs associated with information exchange under this Schedule automatically become part of this Schedule. In order to prevent the need to update Schedule 20 each time a DMA is agreed, each related DMA will need to reflect that it is an Attachment to Schedule 20.

The Schedule also details the relevant points of contact and the escalation processes to be used in the event of a disruption to the agreed access arrangements.

Start Date 5 July 2022

End Date: 5 July 2027

Glossary of Specific Terms

For the purposes of this Schedule, the following definitions apply:

a. A **Claim** is a claim submitted to DVA for compensation, a pension and/or benefit/s under the *Veterans' Entitlements Act 1986 (*VEA*)*, the *Safety, Rehabilitation and Compensation (Defence-related Claims) Act 1988 (*DRCA*)* the *Military Rehabilitation and Compensation Act 2004 (MRCA)*, or the *Australian Participants in British Nuclear Test and British Commonwealth Occupation (Treatment) Act 2006* (BNTBCOF Act).

b. An **Application** is an application submitted to DVA for services, support or benefit other than that provided for under the VEA, DRCA or MRCA

c. **Relevant Acts** are the VEA, DRCA, MRCA or BNTBCOF**.**

d. **Personal Information** Personal information is defined in Section 6(1) of the Privacy Act 1988 as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable:

1) whether the information or opinion is true or not; and

2) whether the information or opinion is recorded in a material form or not.

For the purposes of this Schedule, **Personal Information** includes relevant **Sensitive Information**.

e. **Sensitive Information** is defined in Section 6(1) of the Privacy Act 1988 as:

1) information or an opinion about an individual's:

i. racial or ethnic origin; or

ii. political opinions; or

iii. membership of a political association; or

iv. religious beliefs or affiliations; or

v. philosophical beliefs; or

vi. membership of a professional or trade association; or

vii. membership of a trade union; or

viii. sexual orientation or practices; or

ix. criminal record;

that is also Personal Information; or

2) health information about an individual; or

3) genetic information about an individual that is not otherwise Health Information; or

4) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

5) biometric templates.

f. **Health Information** means**:**

1) information or an opinion about:

i. the health, including an illness, disability or injury, (at any time) of an individual; or

ii. an individual's expressed wishes about the future provision of health services to the individual; or

iii. a health service provided, or to be provided, to an individual;

iv. that is also personal information; or

2) other Personal Information collected to provide, or in providing, a health service to an individual; or

3) other Personal Information collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or

4) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

g. **Staff** means, for the purpose of this Schedule, ongoing and non-ongoing employees, contractors and consultants employed, or engaged, by DVA or Defence.

h. **Authorised Officers** means, for the purpose of this Schedule, those individuals occupying the positions identified in Part I of this Schedule.

PART A: ACCESS REQUIREMENTS

Background

1. Under the 2010 Support for Injured or Ill Project (SIIP), Defence conducted an audit of the systems supporting injured and ill ADF members. While the SIIP report concluded that the support systems were effective, it noted that arrangements were complex and support stove-piped and that further improvements could be made. To that end, the report recommended the development of a coordinated and integrated system of support that extends across both Defence and DVA.

2. The SIIP report made 31 recommendations which were implemented under the retitled Support for Wounded, Injured or Ill Program (SWIIP), a joint Defence/DVA body of work.

3. Included in the 31 recommendations were a number of recommendations aimed at enhancing information management and sharing within and between Departments. Specifically, the report recommended Defence and DVA develop processes and/or technology solutions to enhance sharing of information relating to injury or illness between Departments with a view to streamlining and simplifying claims handling. Work to implement this recommendation is now largely complete.

Purpose

4. This Schedule sets out the arrangements under which Defence and DVA provide access to, or disclosure of, certain Personal Information held in specified Departmental information systems in order to ensure that each Department can effectively and efficiently meet both its statutory and/or functional obligations and commitments under the MoU.

Scope

5. The scope of this schedule is limited to that Personal Information to which access to, or the disclosure of, has been agreed and there is a legitimate basis for such access or disclosure.

6. Further, this Schedule also:

a. sets out the obligations placed on both Departments in respect of the ongoing administration associated with such access or disclosure;

b. establishes an agreed compliance arrangement associated with such access or disclosure.; and

c. details the relevant points of contact and escalation processes to be used in the event of a disruption to the agreed access arrangements.

7. The scope of this Schedule only extends to Personal Information either:

a. held digitally in specified systems or

b. disclosed through the Single Access Mechanism (SAM) in accordance with Schedule 17 to the MoU.

8. To the extent that there is any inconsistency between Schedule 17 and Schedule 20 concerning arrangements for access or disclosure, the provisions of Schedule 20 will prevail. To the extent of any inconsistency between Schedule 20 and the Data Management Agreement between the Department of Defence and the Department of Veterans' Affairs and the Commonwealth Superannuation Corporation of 1 March 2021 (the DMA), the DMA will take precedence.

9. **Exclusion**. The scope of this Schedule excludes the exchange, or disclosure, of personal information held on systems other than those detailed in paragraphs 10 and 12, outside the arrangements detailed in paragraph 11, operationally sensitive information or information in support of Defence housing subsidies which are administered by DVA on behalf of Defence.

DVA Information Requirements

10. To meet DVA's statutory and/or Departmental functional obligations, DVA requires access to, or the disclosure of, Personal Information held in, or sourced from, the following Defence information management systems and/or databases:

a. **Defence One/PMKeyS** to source Personal Information required to:

1) support the determination process for a Claim under one or more of the relevant Acts;

2) determine if a member has rendered Qualifying Service,

3) issue a Non-Liability Health Care White Card

4) finalise an Application, other than a Claim and/or

5) establish a relationship with a member as early in their career as practical.

b. **Safety, Trend Analysis and Reporting Solution (STARS),** to source incident data required to support the determination process associated with a Claim or Application.

c. **Single Access Mechanism Request Management System (SAM RMS)**, to receive electronically information not directly available through system to system access, or where Defence is required to exercise judgement or interpret policy, to support the determination process associated with a Claim or Application.

d. **Defence eHealth System** (DeHS) to source a member's Health Information either following receipt of a Claim or Application or prior to receipt of a Claim or Application but with the member's written consent.

e. **ForceNet**, to facilitate the transfer of large digital files whenever necessary and for communications with ForceNet users.

11. Access to Personal Information in the systems detailed in paragraph 10 is either by system to system integration or individual direct access.

a. **System to System Access**. DVA access to, and Defence's disclosure of, Personal Information held digitally in either Defence One/PMKeyS or STARS or sourced through the SAM RMS, is achieved through secure web services introduced under the Defence DVA Electronic Information Exchange Project (DDEIE) and Single Access Mechanism Request management System (SAM RMS) projects. The arrangements that underpin the disclosure of this Personal Information is detailed in Attachment 1 to this Schedule 20 (Data Management Agreement between The Department of Defence, The Department of Veterans' Affairs and the Commonwealth Superannuation Corporation)(the DMA). The DMA will take precedence over this Schedule 20.

c. **Individual Direct Access.** Individual direct access may be granted to certain Defence systems:

1) **PMKeyS and/or STARS**. Access to PMKeys or STARS requires a DPN account and are accessed through DREAMS. Access is provided in accordance with Annex A, which sets what access specified DVA staff have been granted, and the general terms, conditions associated with that access, and Annex B which details the agreed processes to gain and manage such access.

2) **DeHS and ForceNet**. As DeHS and ForceNet are both web-based platforms, there is no system to system integration between Defence and DVA. As such, access is limited to individually-authorised DVA staff using commercially available Browsers. Access to DeHS or ForceNet is based solely on a DVA staff member's role/need to know and access is to be removed once a staff member no longer has a legitimate need. Access is provided in accordance with Annex A, which sets what access specified DVA staff have been granted, and the general terms, conditions associated with that access, and Annex B which details the agreed processes to gain and manage such access.

Defence Information Requirements

12. Defence requires DVA to discloses to Defence, via system to system integrated web service, details of all claims submitted and, where allowed, the resulting determinations. Details of the

Defence claim and determination requirements and the authority on which such disclosures are made, are set out in the DMA at Attachment 1.

13. Access to DVA ICT systems is limited to the Defence Liaison Officer, access requirements are set out in Work Placement signed on 2 Jun 21 (Attachment 2).

Services Australia (SA) Access

14. Defence and DVA data accessed, or disclosed, under this Schedule, and associated DMAs, will be carried through ICT systems managed and operated by SA as SA is responsible for delivering DVA's ICT services.

15. DVA will work with its ICT provider (SA) to ensure there is no unauthorised or unlawful access by SA staff to the Personal Information of Defence Members, in accordance with the DMA.

PART B: GENERAL TERMS AND CONDITIONS FOR ACCESS

16. The provision of access to, or disclosure of, Personal Information held on a Departmental information system is to be provided in accordance with the Terms and Conditions set out in this Part of Schedule 20.

17. **Privacy**. All access to, or disclosure of, Personal Information held within a Departmental information system must be compliant with the *Privacy Act, 1988* and, where relevant, the DMA at Attachment 1.

18. **Security/Need to Know.** Each Department is individually responsible for ensuring:

a. that access to Personal Information accessed, or disclosed, under this Schedule is only available to staff who have a legitimate need; and

b. all staff who are granted access to data accessed, or disclosed, under this Schedule have, as a minimum,:

(1) the security clearances relevant to the type of access or disclosure:

(a) for information accessed or disclosed under system to system access, the relevant security clearance requirements set out in the DMA at Attachment 1

(b) for individual direct access, the minimum security clearance is a valid Baseline security clearance; and

(2) completed the respective Departmental training in privacy and information security, plus any additional training specified in the relevant Annex to this Schedule.

19. **Relevant Points of Contact**

a. **Individual access**: The relevant Help Desks associated with individual direct access are detailed in Annex C to this Schedule 20. DVA staff are encouraged to use these contacts in the first instance but if there are issues the refer the matter to the Departmental Points Of Contact (DPOC):

(1) Defence DPOC: s47E(d) @defence.gov.au

(2) DVA DPOC: RCG.BSS.data.integrity@dva.gov.au

20. **System to System Information Sharing Arrangements:** the POCs are detailed in the DMA, a copy of which is at Attachment 1.

21. **Dispute Resolution/Escalation Processes**. In addition to the arrangements for dispute resolution set out in the MoU, Annex C to this Schedule 20 details the agreed dispute resolution escalation processes applicable to the provision of access to, or disclosure of, Personal Information.

22. **Individual Direct Access Account Sponsorship**.

a. **DPN, PMKeyS, STARS, DeHs and ForceNet**. As only DVA can verify an applicant's need to access to the DPN, PMKeyS, STARS, DeHS or ForceNet, and confirm that the applicant has the necessary security clearance and has completed all prerequisite training, the DVA POC is to sponsor all DVA requests to create, modify and cancel user registration requests..

b. **DVA ICT systems**. Arrangements to support access to the DVA ICT systems for the Defence Liaison Officer are set out in the Agreement between the Department of Defence and the Department of Veterans' Affairs for Work Placement signed on 2 Jun 21.

23. **Individual Direct Access Management**. Each Department is to ensure appropriate management arrangements are put in place to:

a. manage individual access to the other Department's information systems, including the submission of all applications to the relevant authority, and the recording of related information including the individual's details, the specific access required, the date access is first required and any subsequent changes in individual access requirements including the cessation of an individual's legitimate need for access;

b. inform the providing Department of all changes to staff access granted under subparagraph 23a, including changes in individual access requirements and the cessation of an individual's legitimate need for such access;

c. track the allocation, within the respective Departments, of access tokens and/or any other hardware provided by the host Department;

d. advise the other Department of the allocation and return of all access tokens to allow for the disassociation of each token from the relevant account, and the secure storage until they can be reallocated;

e. immediately report any security or privacy breaches associated with access under this Schedule to the other Department;

f. conduct regular random auditing of access to the other Department's information systems to confirm that all requirements of the *Privacy Act 1988* (the Privacy Act), including Schedule 1 of the Privacy Act being the 13 Australian Privacy Principles, and this Schedule are being complied with;

g. report the results of such audits to the other Department's POC including any security or privacy breaches and the resulting action; and

h. provide the other Department information and data necessary to fulfil their obligations under this paragraph.

24. **System to System Access Management.** Access management for Personal Information disclosed through system to system integration is in accordance with the DMA at Attachment 1.

25. **Stakeholder Engagement**. The Department responsible for the collection, storage and management of Personal Information that is subject to access or disclosure under this Schedule is to:

a. formally recognise the other Department as a key stakeholder in the management of the relevant information system and/or access and disclosure arrangements;

b. ensure the other Department is advised of all proposed process and procedural changes that may impact their access to or use of systems, or impact their responsibilities under this Schedule, prior to the implementation of any change within a reasonable period to provide input into any change and prepare for any changes to business or other processes; and

c. ensure that the other Department is consulted on system changes that impact their use of the system ahead of any system change within a reasonable period to provide input into any change and prepare for any changes to business or other processes

PART C: FACILITIES AND ACCOMMODATION REQUIREMENTS

DVA Standing Requirements

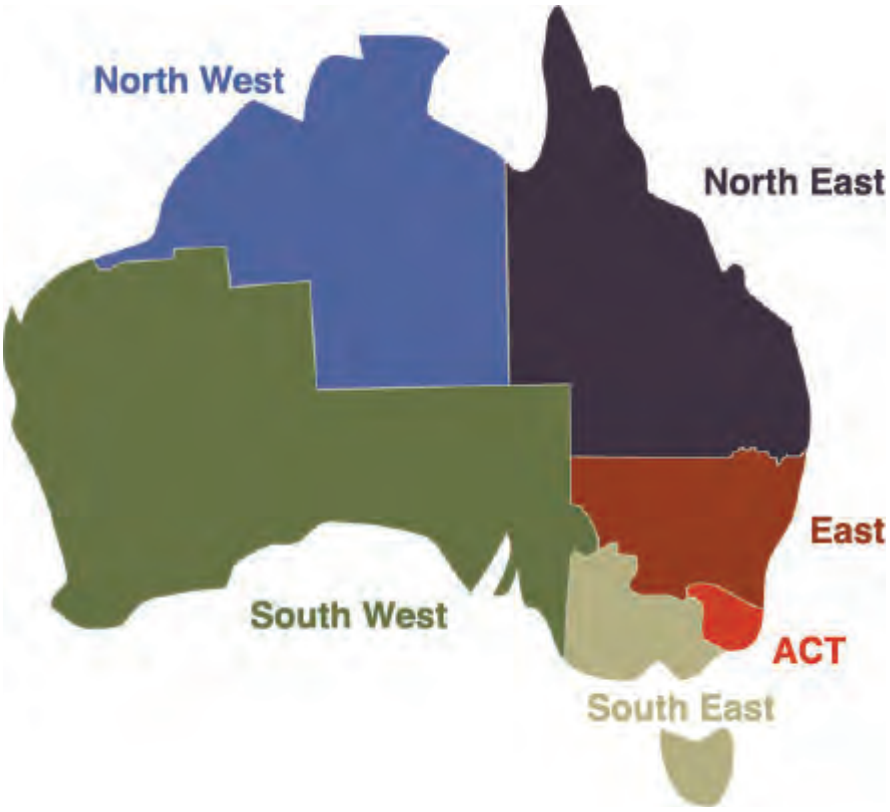
26. Select DVA staff have a standing requirement to access current and former ADF members' Personal Information held by Defence where they have the member's informed consent or where permitted under legislation. Access to this information can be achieved through the DPN either from a workstation on a Defence establishment or via remote access through the use of DREAMS.

27. Remote access to either DREAMS or DVA ICT systems may not be possible from all Defence facilities, due either to the physical nature of the facility or for security reasons, and may require the provision of a dedicated DPN desktop Personal Computer (PC) in standard configuration.

28. All applications by DVA for a dedicated DPN desktop PC in standard configuration are to be requested via the CIOG ICT Service Request Catalogue. Access to the DPN CIOG ICT Service Request Catalogue can be found at s47E(d)

29. Alternatively, DVA can seek support from the relevant team from Defence's Directorate of Regional ICT. Details of the regional points of contact are:

a. ACT : s47E(d) @defence.gov.au
b. East: s47E(d) @defence.gov.au
c. North East: s47E(d) @defence.gov.au
d. North West: s47E(d) @defence.gov.au
e. South East: s47E(d) @defence.gov.au
f. South West: s47E(d) @defence.gov.au



30. On receipt of such an ICT Service Request, CIOG is to arrange for dedicated access to a DPN desktop PC in standard configuration providing it is practical to do so.

31. Desktop PCs are to be located within the on-base workspace allocated by Defence for use by DVA staff. The costs associated with the provision of DPN desktop PCs remain the responsibility of DVA unless otherwise agreed.

32. Should CIOG determine that the provision of dedicated access to a DPN desktop PC is not practical for any reason, CIOG should liaise with the applicant to determine an alternate solution, including the provision of a Defence Protected Laptop. Costs associated with the implementation of an alternate solution remain the responsibility of DVA.

Defence Requirements:

33. The only Defence facilities and/or accommodation requirements under this Schedule are in relation to the Defence Liaison Office and are detailed in the Agreement between the Department of Defence and the Department of Veterans' Affairs for Work Placement signed on 2 Jun 21.

PART D: FUNDING RESPONSIBILITY

34. Access to, or the disclosure of, personal information under this Schedule is to be provided at no cost to the Department seeking the information.

35. Noting the agreement to consult on systems changes under paragraph 25 of this agreement, the cost associated with the development, modification, provision, licencing and/or installation of any hardware, software or web services necessary to facilitate such access, or disclosure, is the responsibility of the Department seeking the information unless otherwise agreed.

36. Where applicable, the cost associated with the provision of hardware and software remain the responsibility of the requesting Department but is to be in accordance with the providing Department's standard internal pricelists/charges. All initial hardware and software costs are to include ongoing support.

PART E: PERSONNEL REQUIRED

37. There are no additional personnel requirements associated with this Schedule.

PART F: MONITORING AND EVALUATION

38. The Authorised Officers are responsible for ensuring that this Schedule is reviewed, and amended where required, at least annually from the commencement date to ensure its continued validity and accuracy. A summary of each annual review is to be provided to the Defence DVA Links Steering Committee.

PART G: PERFORMANCE MEASURES AND STANDARDS

39. There are no specified performance measures or standards applicable to this Schedule.

PART H: SPECIAL PROVISIONS

40.

41. The Parties agree that during the term of this Schedule 20, Attachments can be agreed between the Parties and once signed by both Parties' Authorised Officers, automatically form part of this Schedule 20 as the next numbered Attachment.

PART I: AUTHORISED OFFICERS AND ADDRESSES FOR NOTICES

42. The Authorised Officers for this Schedule are:

	Defence	DVA
Position	Director General Veterans' Support	Assistant Secretary Claims Assessment and Management
Postal Address	s47E(d) Brindabella Park Offices PO Box 7927 Canberra BC ACT 2610	GPO Box 9998 Brisbane QLD 4001
Telephone	s47E(d)	s47F
E-mail	s47E(d) @defence.gov.au	s47F @dva.gov.au

Signatures

Signed for and on behalf of the Department of Defence by the Director General Veterans' Support

s47E(d)

Date: 2022.07.05 14:33:23 +10'00'

Signed for and on behalf of the Department of Veterans' Affairs by the Assistant Secretary Claims Assessment and Management

_____ __/__/__

Annexes:

A. Defence Information Systems To Which DVA Has Been Granted Access
B. Agreed Processes To Access to Defence Information Systems
C. Help Desk Points Of Contact And Escalation Processes
D. Authorised Sponsors

Attachments:

1. Data Management Agreement between The Department of Defence, The Department of Veterans' Affairs and the Commonwealth Superannuation Corporation
2. Agreement between the Department of Defence and the Department of Veterans' Affairs for Work Placement signed on 2 Jun 21

Annex A
To Schedule 20 of
Defence/DVA MoU

DEFENCE INFORMATION SYSTEMS TO WHICH DVA HAS BEEN GRANTED ACCESS

1. This Annex details the Defence Information Systems to which DVA has been granted access and sets out the approved level of access. This Annex may be amended by agreement of the Authorised Officers to reflect changes in the type and level of access without the need to re-sign the Schedule.

2. DVA access to and the disclosure of Personal Information from, Defence Information Systems is either through system to system integration or via Individual Direct Access.

System to System Integration

3. The Defence DVA Electronic Information Exchange Project (DDEIE) has integrated select DVA ICT systems with PMKeyS and the Safety Tracking, Analysis and Report Solution and provide a Very Large File transfer capability while the Single Access Mechanism Request Management System Project has integrated the DVA request and Defence response functions. Full details of the access to, and disclosure of, Personal Information through this system to system integration is set out in the DMA at Attachment 1.

Individual Direct Access

4. **Defence Protected Network (DPN)** Access to Defence One/PMKeyS requires access to the DPN using a DREAMS token. Details of how to gain access to the DPN is set out in Annex B. DVA access to the DPN is as follows:

Access Profile	**Basis**	**DPN Roles**	**Access Granted**	**Restrictions**	**Comments including mandatory training**
DPN	Access granted to DVA staff with legitimate access requirements	DVA Access	Corporate Directory; Pay and Conditions; ADF Pay & Conditions Manual (PACMAN); ADFPAY; Defence Force Remuneration Tribunal (DFRT); DEFGRAMs; Defence Force Salary & Allowance Accounting Circulars (DEFSAACs); and Army manual.	Read only (including Print/Export)	Nil
			Intranet, MS Outlook, Word, Excel, and Campus.	Full	
			CAMPUS	Full	For access to training courses

5. **Access to Defence One/PMKeyS.** Access to Defence One/PMKeyS is granted to select DVA Staff to allow them to verify the validity of a Claim or Application and to source relevant data to allow a DVA delegate to make a determination in relation to a Claim or Application. Access is granted under two discrete profiles, one associated with the payment of military compensation and the other in relation to the determination of a claim. Details of how to gain access to Defence One/PMKeyS is set out in Annex B. DVA access is as follows:

Access Profile	Basis	Defence One/PMKeyS Roles	Access Granted	Restrictions	Comments including mandatory training
DVA SAM	'Browser' access is granted to approved DVA staff to allow them to confirm the validity of a request submitted to DVA. This access allows approved DVA staff to view Job Data, Op Log, Pre-PMKeyS Service Details and Individual Readiness. They do not have access to emergency contacts, leave or pay data. Once approved DVA staff have confirmed that the client is a bonafide claimant they will then raise paperwork via Defence SAM team to investigate further if required.	MAP1_R_DVASAM	Individual Readiness	Read only (including Print/Export)	Nil
			Operational Log		Nil
			Pre- PMKeyS data		Nil
			Contract data		Nil
			Accomplishment History		Nil
			Job data		Nil
			TrainingTraining		Nil
			Student Training		Nil
			Attendance History Summary		Nil
			Training Day Balance Summary		Nil
		HCP1_R_DVASAM	ADO Employee Pay Attributes		Nil
		MAA1_R_DVASAM	Archived Data		Nil

6. **Access to Work Health Safety (WHS) Data**. Access to the Safety Trend Analysis and Reporting Solution (STARS) is granted to select DVA staff to allow them to access Defence data relating to a WHS event relevant to the determination of a Claim or Application. Details of how to gain access to STARS is set out in Attachment B.

Access Profile	Basis	STARS Roles	Access Granted	Restrictions	Comments
STARS	Access granted to allow approved DVA staff to access event reporting relevant to claims under consideration by DVA.	DVA SAM	Defence data within STARS including Personal Information.	Read Only (Including Print/Export)	Nil

7. **Access to Defence Organisation's Corporate Learning Management System** (CAMPUS). Users with DPN access will automatically have access to CAMPUS.

8. **Access to the Defence eHealth System (DeHS**). Access to DeHS is granted to select DVA staff to allow them to access Defence Health Information relevant to the determination of a Claim or Application. Details of how to gain access to DeHS is set out in Annex B.

Access Profile	Basis	DeHS Role	Access Granted	Restrictions	Training Required	Comments
DeHS	Access granted to DVA Staff to facilitate consideration of a Claim or Application.	DVA	Consultation data	Read Only (Including Print/Export)		
			Medical Records	Read Only (Including Print/Export)		
			Confidentiality Policies	Override Policy Only		

9. **Access to ForceNet.** Access to ForceNet is granted to select DVA staff to allow File sharing between the DCO and the DVA Single Access Mechanism (SAM) teams and DVA (including Open Arms) communications with ForceNet users.

a. In both cases, DVA staff registered on ForceNet will be provided a permanent user account but are to limit their use of ForceNet to the Group associated with the basis for their access. DVA staff registered on ForceNet are not to seek to join any other ForceNet groups without specific approval from the ForceNet Capability Coordinator.

b. **ForceNet File Transfer.** Prior to the introduction of the Single Access Mechanism Request Managements System (RMS), approval was granted for the use of the existing file transfer capability within the ForceNet application to expedite the sharing of files (up to Official/DLMs) with select staff employed within DVA (and CSC). File sharing is actioned through a dedicated closed group within ForceNet. Following the introduction of the RMS, file transfer via ForceNet will be retained as a backup to the integrated solution.

(1) Membership of this group will controlled by the Assistant Director, Defence Single Access Mechanism (SAM) and limited to:

i. Defence SAM users, consisting of Australian Public Service (APS ongoing and non-ongoing) and contractors (with ODS numbers).

ii. Invited DVA SAM team members, consisting of APS and contractors working within the DVA SAM Team.

(2) Defence SAM is responsible for creating and managing the closed professional 'ForceNet Defence SAM – DVA' group with 'Members Only' access and for sponsoring DVA SAM staff registration on ForceNet.

(3) The DVA POC is responsible for verifying that DVA staff applying for ForceNet registration are employed in the DVS SAM team and have a genuine business need for such access.

(4) Procedure for file transfer using ForceNet are in Appendix 1.

c. **DVA Use of ForceNet for Communications.** Defence has approved select DVA staff employed in either the DVA or Open Arms Communications teams to be registered as ForceNet users, with a permanent user account, in order to exploit ForceNet as an additional communications channel for information on services and support available from DVA and Open Arms. The DVA POC is responsible for verifying that DVA staff applying for ForceNet registration are employed in either the DVA Communications team or the Open Arms Communications team and have a genuine business need for such access.

10. **Access CAMPUS**. Objective and CAMPUS are available to all DPN users. CAMPUS access is unrestricted, DVA access to Objective will be limited by Objective folder permissions. The Assistant Director Defence SAM is responsible for arranging folder access for DVA staff with folder owners.

Appendix 1
To Annex A
To Schedule 20 of
Defence/DVA MoU

PROCEDURE FOR FILE TRANSFER USING FORCENET

1. The procedures for file transfer using ForceNet are:

a. DVA requests relevant information to assist with the determination of member's liability from Defence SAM through the Request Management System.

b. Defence SAM requests information from relevant areas within Defence

c. Areas in Defence send requested information to Defence SAM.

d. Defence SAM compiles the information into a PDF document and password protects.

e. Defence SAM uploads PDF document to the private DVA shared file area (100mb limit per PDF document).

f. Defence SAM sends email notification to DVA, that files have been uploaded.

g. DVA user logins to ForceNet and downloads the files.

h. DVA user deletes the files.

i. DVA user log out of ForceNet.

2. To expedite the transfer of files from Defence to DVA, the Assistant Director, Defence SAM may authorise other Defence users to upload documents directly to the private DVA shared file area in which case the authorised Defence user is responsible for sending the notification email to DVA and Defence SAM.

3. DVA agrees to download and delete files transferred using ForceNet within three working days of receipt of email notification.

4. In accordance with direction from Defence ICT security, ForceNet Administration will delete all documents uploaded into ForceNet seven calendar days after upload irrespective of DVA obtaining the documents or not. Access to deleted files will be the subject of a new request from DVA.

Annex B
To Schedule 20 of
Defence/DVA MoU

AGREED PROCESSES TO ACCESS TO DEFENCE INFORMATION SYSTEMS

Agreed Process

1. The agreed process for gaining access to and reporting issues with Defence services are outlined in the following Defence documents:

- *"DVA - Accessing Defence Services"*
- *"Part 1: DVA Issue and Contact Details - INM Process for DVA Users of Defence Services"* provides contacts and the process to follow when an individual user has issues with Defence services.
- *"Part 2: DVA Issue and Contact Details - INM Process for Support Providers of Defence Services"* provides contacts and the process to follow when communicating or escalating issues with Defence services. The audience for this document is intended for DHS and Defence Service Desks; and DVA Support Teams (only).

2. The Defence POC is responsible for providing the DVA POC with copies of the current versions of the above documents.

DPN Access

3. Requests for DPN access must be made to the DVA POC who submists the requests to Defence on their behalf. The DVA POC must confirm that the required security clearance is held by the DVA staff prior to requesting access.

4. Process for DVA Staff to access DPN.

- DVA officer applies for Baseline Security Clearance(as a minimum) from AGSVA via the DVA Security team.
- Once Clearance gained, provide evidence to DVA POC.
- DPN Access applied for by DVA POC. To arrange access to the Defence Protected Network, the DVA POC (with DPN access) accesses the search facility of the Defence ICT Services Catalogue, enters 'Electronic new account request' and follow the prompts. If the ICT Service Catalogue is not available please call the ICT Service Desk on (0) 133 272.
- DPN Access gained.

5. The DVA POC must advise the Defence POC if a DVA user no longer requires access to DPN.

6. Issues with access to the DPN are to be addressed through the ICT Service Centre using the Log A Job Online or by calling the ICT Help Desk on 133 272.

DREAMS Tokens

7. DREAMS tokens are provided by Defence to the DVA POC. The DVA POC is responsible for distributing tokens the relevant DVA staff. As Dreams tokens are provided by

Defence to DVA in bulk, and not to individuals, the DVA POC should request additional tokens through the Regional ICT team.

8. An alternative to the use of a DREAMS token is the DREAMS token application which can be applied for by an individual once they have a DPN account via Log a Job Online. Once a Dreams Token Application has been received, the physical Dreams token must be returned to DVA Corporate Services for reissue to new staff as required. Note that the Dreams Token App is currently only available for iPhones/Ipads.

9. Details of the DREAMS token issued to the DVA user must be recorded for audit purposes and available to Defence upon request. Upon receipt of the DREAMS token the DVA user is required to activate the token by contacting the ICT Service Desk on 133 272.

10. When a DVA user no longer requires access to the DPN, the DVA Corporate Services must recover the DREAMS token from the user and hold securely for reallocation as required. The DVA DPOC is to then request that the user's DPN account be cancelled via the following DPN link:

s47E(d)

11. The DVA user must advise the DVA POC and the Defence ICT Service Desk 0) 133 272 if a DREAMS token is lost, faulty, expired, or flat battery. For lost tokens, the use is to complete an XP188 Security Incident Report. Assistance may be sought from the relevant Defence Regional ICT POC if needed.

12. DREAMS connectivity issues affecting a DVA site or whole agency must first be reported to the DVA service provider (i.e. Services Australia) for investigation.

Defence One/PMKeyS Access

13. Defence One/PMKeyS access is only granted if relevant CAMPUS training has been completed successfully and an access application form is submitted with evidence of the completed training and security clearance attached.

14. Process for DVA Staff to obtain Defence One/PMKeyS Access

- DVA users complete the following Defence One/PMKeyS training via CAMPUS:
  - Australian Privacy Principles eAssessment ID#00007392.
  - Defence One/PMKeyS Introduction and Reporting ID#00004761.
  - Defence One/PMKeyS Introduction to Global Payroll ID#00004763
- DVA Defence One/PMKeyS access application (AD688 Application for PMKeyS Access) completed by DVA user and sent to DVA POC who will complete as supervisor and forward to People Systems Business Support (PSBS) Access Management at s47E(d) @defence.gov.au . Application must include attached evidence of completed training and Security Clearance.
- Defence One/PMKeyS access processed by the PSBS Access Management.
- DVA user and DVA POC notified by the PSBS Access Management of access.
- DVA user commences transacting within Defence One/PMKeyS.
- Issues with access to the Defence One/PMKeyS must be reported using the agreed process.

15. When DVA staff access to Defence One/PMKeyS is no longer authorised the relevant DVA Supervisor is to send an email to s47E(d) @defence.gov.au.

STARS Access

16. Read Only access to the Safety Trend Analysis and Reporting Solution (STARS) will be granted to DVA staff who have been approved by the DVA POC.

17. Defence will maintain a list of approved DVA staff and the DVA POC will advise of any alterations via email to WHS.STARS@Defence.gov.au.

DeHS Access

18. DeHS access is achieved via an Internet connection to the URL https://www.jehdi.com.au. Access to DeHS itself requires secure credentials that are obtained via the DPN ICT Service Desk.

19. Access to DeHS is obtained as follows:

- A DeHS New Account request is to be submitted with the DVA POC listed as the approver.
- Training / Sandbox logon credentials are issued to the user and the DVA POC.
- Once defined training, available within the Training Environment, has been completed the user is to submit a JeHDI Production Account Activation request listing s47E(d) @defence.gov.au as the authoriser.
- Production account passwords will be distributed and the user will be granted access to DeHS.

20. The DVA POC is to advise the DeHS Business Support Team of access adjustments immediately either via email at s47E(d) @defence.gov.au or via phone on (02) 6127 0001.

ForceNet Access

21. Access to ForceNet is dependent on the type of access being sought. The DVA POC is to verify that DVA staff seeking to be registered as a permanent user on ForceNet, either to utilise the ForceNet file sharing capability or for general communications, have a genuine business need and understand the limitations and conditions associated with being a registered ForceNet user.

22. Once verified, the DVA POC is to send the registration request to the ForceNet Capability Coordinator at s47E(d) @defence.gov.au.

23. Registration requests must contain the following details for each DVA staff member to be registered on ForceNet:

- **Full name:**
- **ODS/Employee ID number: Department of Veterans' Affairs Employee**
- **Date of Birth: DD/MM/YY**
- **Contract provider/company: Department of Veterans' Affairs**
- **Work phone number:**
- **Email address: work email address**

- **Security Clearance: Baseline**
- **End date for the contract: Access will cease on this date or two (2) years from the date of access, whichever is first;**
- **Business reason for requesting access to ForceNet: File transfer between DCO (Defence SAM) and DVA or Open Arms for communications with ForceNet users. (***delete whichever is not required).*
- **DVA Internal Sponsor: The DVA POC.**

24. On receipt the ForceNet Capability Coordinator verify that the applicant/s hold the necessary security clearance.

25. **Defence Sponsorship**. Where the request is to support file sharing, the ForceNet Capability Coordinator will seek agreement from the Assistance Director, Defence SAM to sponsor the application. For applications associated with communications, the ForceNet Capability Coordinator will sponsor applications.

26. Once the applicant/s security clearance and Defence sponsorship is confirmed, ForceNet Capability Coordinator will authorise the creation of an account for each applicant. ForceNet Admin will then email each applicant details on how to register on. For File Sharing accounts, the email detailing how to register will be cc'd to Assistant Director Defence SAM.

27. **File Sharing**. Once the authorised DVA users have registered with ForceNet, and advised the Assistant Director Defence SAM, they will be invited to join the Defence SAM – DVA group to gain access to the shared files. Only invited users to this specific professional group are allowed to access the shared files.

28. **Communications.** Once the authorised DVA users have registered with ForceNet they will be able to access the relevant group page (DVA or Open Arms) and post communications.

Annex C
To Schedule 20 of
Defence/DVA MoU

HELP DESK POINTS OF CONTACT AND ESCALATION PROCESSES

Help Desk Points of Contact

1. Initial points of contact for access or disclosure issues are the relevant help desk:

a. **System to System Integration.** The Help Desks for each of the information flows are detailed in the DMA at Attachment 1 to Schedule 20.

b. **Individual Direct Access**. Help Desks for staff with individual direct access to Defence Information Systems are:

Department	System	Initial Assistance	Further Assistance	Escalation
Defence	DPN	Services Australia (Gateway owners) Service Desk on 1300 300 710 SA Service Desk will log the incident with the Defence ICT Service Desk (0) 133 272 if not a SA gateway error.	DVA POC (RCG.BSS.data.integrity@dva.gov.au	Referral by the Defence ICT Service Desk to next level
	DREAMS Connectivity	Services Australia (Gateway owners) Service Desk on 1800 264 467,	Defence ICT Service Desk (0) 133 272 noting SA Service Desk will log the incident for DVA if not a SA gateway error. DVA POC (RCG.BSS.data.integrity@dva.gov.au)	Referral by the Defence ICT Service Desk to next level
	Defence One/ PMKeyS	Defence Service Centre 1800 333 362	PMKeyS Customer Support Centre (PCSC) referral by Defence Service Centre.	Defence POC
	STARS	Sentinel Help Desk 1800 220 820	Referral by Sentinel Help Desk To next level	Defence POC
	Defence Email Accounts	Defence ICT Service Desk (0) 133 272	Referral by the Defence ICT Service Desk to next level	Defence POC

	DREAMS Access Request	DVA POC	Defence Regional ICT teamDeren	Defence DPOC
	Lost DREAMS token	Notify DVA POC and the Defence ICT Service Desk (0) 133 272 to disable the token. Complete XP188 Security Incident Report.	Another DVA member with a DREAMS token can lodged the Security Incident Report on behalf of another. Report the incident to the DVA POC (RCG.BSS.data.integrity@dva.gov.au). Obtain another token from the DVA POC .	Defence POC
	Faulty, expired, flat battery	DVA POC Defence ICT Service Desk (0) 133 272 to disable the token.	Obtain another token from the DVA POC who arranges return of token to Defence via relevant Defence Regional ICT team.	relevant Defence Regional ICT team.
	DeHS	Defence ICT Service Desk (0) 133 272 for IT issues	DeHS Business Support Team on s47E(d) @defence.gov.au or (02) 6127 0001 for System / Process / Permissions issues	Defence POC
	ForceNet	1800 Defence	ForecNet@defence.gov.au	Defence POC

Escalation

2. Existing reported disputes or issues should be escalated, in the first instance, through relevant Defence area (e.g. ICT Service Desk) advising that a reported dispute or issue remains unresolved; or the impact has changed.

3. If, after escalation through the relevant help desk, a dispute or issue cannot be resolved then the matter will be referred to the Defence POC. The referral should include actions to date and an impact statement.

4. If the Defence POC is unable to resolve the issue, the matter will be referred Director General Veterans Support in Defence and the Assistant Secretary Claims Assessment and Management Branch in DVA.

5. If the issue is still unable to be resolved, the matter will follow the process for ‘Managing Issues Between The Parties’ set out at clause 30 of the MOU.

Annex D
To Schedule 20 of
Defence/DVA MoU

AUTHORISED SPONSORS

1. Certain positions in Defence and DVA are authorised to sponsor candidates for access to systems in the other Department. It is the responsibility of the sponsor to ensure that a candidate meets all the requirements for access to the system or systems in question, including but not limited to a legitimate need to access personal information, are aware of their obligations and responsibilities and possess the appropriate level of security clearance. The sponsor will ensure the candidate completes the relevant parent Department training in privacy and information security, plus any additional training specified in either Annex A or B as appropriate.

2. The decision to grant access to a candidate, however, will remain with the department which owns the system in question regardless of sponsorship. It will be expected, however, that in the normal course of events, a sponsored candidate, meeting all the requirements for access to a system, will be granted access by the owner of the system.

3. In DVA, the DVA POC is the sponsor for all DVA staff access to Defence systems. Issues with accessing Defence systems should be addressed in accordance with Annex C.

4. As the only Defence member requiring access to DVA ICT Systems is the Defence Liaison Officer, there is currently no need to promulgate a Defence sponsor.