Proposal to Department of Veterans' Affairs for Automated Straight-Through and Streamlined Processing

Gov Law Tech Services Pty Ltd

November 1, 2016

Contents

1 Introduction

We are pleased to present a proposal to deliver a production-ready, cloud-based, open source, technology system for automatically determining liability under DVA's

1. Straight-Through Processing procedures for MRCA claims for post-30 June 2004 enlistees.
2. Streamlined processing produces for MRCA and VEA claims.

This is designed to:

1. Yield measurable reductions in the average time for veterans to get access to treatment and rehabilitation.
2. Integrate into DVA's existing and future claims processing pipeline.
3. Reduce human error and improve consistency in the way DVA administers the law.

The broader objective is to help DVA:

- Deliver on the Minister for Veterans' Affairs intention to "reduce the time taken to process claims and make the claims process easier and more stress free for our veterans."[1]
- Further the objectives of Veterans Centric Reform.
- Execute the Secretary's 2020 vision to "continue to expand the electronic data exchange between DVA and Defence, allowing for the automatic validation of service history data...and work together to develop plans for pre-population of Defence information into new claims, further improving the user experience".

Gov Law Tech is well placed to deliver this system, having completed two pieces of work for DVA previously:

- Fixed Price Advisory work on migrating executable business rules in the Defcare application to open platforms – advice considered by the Improving Processing Systems team as part of its work on improving the processing of Incapacity Payments.
- Time and Materials Development work as part of the Lighthouse Project.

[1] Media Release of 15 September 2016, The Hon Dan Tehan MP

2 Proposed Solution

We propose to deliver an automated decision service that helps determine the connection between condition and service by automatically applying SoPs according to DVA-defined rules. For all conditions for which there is a SoP in effect, the solution provides the relevant SoP factors a delegate needs to consider. For conditions for which DVA has defined rules for when particular SoP factors are satisfied, the solution takes the further step of determining the full connection to service.

Key business features are:

- The system automatically updates within one business day – without human intervention – SoP factors and conditions when Statement of Principles registered on the Federal Register of Legislative instruments come into effect.
- For each case, the system produces an editable case summary as Microsoft Word document setting out the applicable SoP factors and satisfied SoP factors, to assist delegates to make a determination.

The main technical features are:

- The System will be accessible via a simple web-based Application Programming Interface (API). This means the System is designed to be integrated into other software components – both existing systems in DVA such as the Integration Support Hub, MyAccount and MyService, and future systems.
- The source code will be under the Apache 2.0 licence. This means, broadly, that DVA, other agencies, and any other parties may use the source code for any purpose without fees or licensing complications.
- The System will run on the Java Virtual Machine, a platform with with DVA is familiar and experienced.
- The System does not store or require any personal information under Australian privacy regulations.
- The System is designed for deployment to a managed hosting provider from the Department of Finance's Cloud Services Panel certified by the Australian Securities Directorate to FOR-OFFICIAL-USE-ONLY level. This enables DVA to deploy and maintain the system for a fraction of the cost and time involved in using DHS

Shared Services Centre infrastructure.

3 Benefits

The solution is the core of a system to apply Automated Streamlined and Straight-Through processing. The benefits of an automated approach to Streamlined and Straight-Through processing are:

- The correct SoP for given condition is automatically identified virtually instantly, eliminating the chance of applying the wrong SoP or the wrong version of a SoP.
- The system reliably and quickly performs date arithmetic to conflate periods of operational and non-operational service for the purpose of determining the appropriate SoP to apply, saving delegate time and reducing the risk of error.
- DVA can implement policy changes for Streamlined and Straight-Through processing more quickly – the changes only require code changes as apposed to delegate training, policy manual updates and other business process changes.

The solution is likely to result in substantial quantifiable improvements in the average time to determine initial liability for MRCA claims. The average time to determine initial liability for MRCA claims was 109 days in 2014-2015 [2]. We estimated DVA expended approximately $21.6M on administering MRCA claims in 2014-2015[3]. Automated Straight-Through Processing and Streamlined Processing has the potential to make a significant positive impact on this time and spend, given:

- Over 50% of MRCA claims are for wear and tear injuries, which are amenable to Straight-Through processing.
- DVA's Rehabilitation and Support group has nominated a high critical error rate due to the wrong instrument used, outdated content on SoP factors, time spent authoring decision letters and a lack of IT system support for Streamlined conditions as impediments to faster processing - all issues this solution addresses.

[2] DVA 2014-2015 Annual Report, page 56

[3] Administered dollars for MRCA and SRCA allocated to MRCA in proportion to number of claims, see page 56 of 2014-2015 Annual Report

To be effective, the solution needs to be integrated into DVA's existing claims processing IT systems. The solution is designed to be as easy as possible to integrate:

1. The solution involves simple web-based services which can be consumed by multiple different technologies and applications, both existing and future.
2. The solution does not require or store any personally identifiable data or claims records.
3. All code in the solution is open source and runs on the Java platform with which DVA is familiar, to facilitate amendment and maintenance by DVA personnel.
4. The solution is capable of running securely on DVA, DHS or highly economical cloud infrastructure (the latter being recommended).

4 Components

The solution consists of two components:

- The **SoP Support Service** applies condition-specific rules to a veteran's service history data to help determine whether condition is related to Defense service according to the relevant SoP.
- The **SoP Reference Service** provides up-to-date information about SoP factors, conditions, and operations.

These components are designed to be consumed directly by other computer software components.

DVA may exploit the SoP Reference Service independently from the SoP Support Service. The SoP Support Service has a runtime dependency on the SoP Reference Service.

4.1 SoP Support Service

The SoP Support Service helps delegates determine whether:

1. A particular condition of a given veteran who enlisted after 30 June 2004 is related to Defense service under subsection 338(3) (Reasonable

Hypothesis) or subsection 339(3) (Balance of Probabilities) of the Military Rehabilitation and Compensation Act 2004 ("**Straight Through Processing**").

2. A particular condition of a given veteran qualifies for **streamlining procedures** under the MRCC streamlining policy applying to MRCA and VEA claims.

4.1.1 Inputs

The SoP Support Service expects the following inputs for each determination:

1. **Condition Data**:
    - Identification of the condition by a SoP condition name and/or ICD code.
    - Indication of whether the condition is acute, or accumulated over time ('wear and tear').
    - A date or date range in which the condition onset occurred.
    - Additionally, for aggravation/worsening claims: the date or date range in which the aggravation occurred.
2. **Service history data**.

The expected service history data is:

1. Date of Enlistment and Separation
2. Original Hire Date
3. A list of services in which the veteran has served, including
    (a) Service Name (e.g., 'Royal Australian Air Force')
    (b) Service Type (e.g., 'Regular/Permanent Force')
    (c) Start Date
    (d) End Date
4. A list of the veteran's operations, including:
    (a) The operation name
    (b) The start date
    (c) The end date

(d) The dates for which the veteran was within the 'Specified Area' under determinations of the Chief of the ADF under paragraph 6(1)(b) of MRCA.

> **Note**
>
> This data is a strict subset of the data currently accessible to DVA under the 2015 Defence-DVA Data Management Agreement for Qualifying Service.

An example of the expected service history data is:

```
{
  "serviceSummaryInformation": {
    "originalHireDate": "2004-07-01Z"
  },
  "serviceDetails": [{
    "service": "Royal Australian Air Force",
    "serviceType": "Regular/Permanent Force",
    "startDate": "2004-07-01Z",
    "endDate": "2016-01-01Z",
    "operationalService": [
      {
        "assigned": "2006-07-01Z",
        "description": "Operation WARDEN",
        "event": "Within Specified Area",
        "startDate": "2006-07-10Z",
        "endDate": "2007-07-01"
      },
      {
        "assigned": "2009-07-01Z",
        "description": "Operation RIVERBANK",
        "event": "Within Specified Area",
        "startDate": "2009-07-10Z",
        "endDate": "2010-07-01Z"
      }
    ]
  }]
}
```

4.1.2 Processing

The SoP Support Service automatically applies rules to determine an outcome, given only the input data listed above. The Service will apply rules from both DVA's 'Straight-Through Processing' and 'Streamlined Processing' policies in the same way.

The rules will operate according to the following logic:

1. Firstly, determine the applicable SoP factors for condition, given the Condition Data listed above. This involves identifying the correct SoP instrument.
2. Secondly, determine satisfied SoP factors according to defined rules, if any (see below).
3. Thirdly, for SoP factors that involve a quantitative threshold, determine the veteran's progress towards or beyond this threshold, according to defined rules, if any (see below).

The logic to determine applicable SoP factors is as follows:

Condition Type	**Date of Onset**	**Aggravation /Worsening***	**Logic to determine whether Balance of Probabilities (BoP) or Reasonable Hypothesis (RH) SoP applies**
Acute	Exact	No	If the date is in a period when the veteran was on operational service: RH. Otherwise: BoP.
Acute	Range	No	If the veteran was on operational service in at least 50% of the days in the given date range: RH. Otherwise: BoP.
Wear and tear	Either	Either	According to a rule specified by DVA for each factor.

* contracted before or during (but not arising out of) the person's relevant service.

DVA is to provide Gov Law Tech with specifications for rules for:

- 'Wear and tear' conditions (Straight-Through Processing)

- Streamlined Processing conditions (listed at Appendix A)

Each rule specification must:

- Identify the relevant SoP instrument by either the unique ID of the authorised version from the Federal Register of Legislative Instruments or the number and year from the citation.
- Identify the SoP factor or factors which are inferred to be satisfied based on the rule, including the unique ID of the authorised instrument from the Federal Register of Legislative Instruments. (Corresponding factors from Balance of Probabilities and Reasonable Hypothesis SoPs are considered separate factors.)
- Describe how to infer whether the factors are satisfied based solely on the data listed in 'Inputs' above.

In addition, for SoP factors which contain a quantitative threshold (such as number of kilograms lifted), the specification may contain an average rate of accumulation towards that threshold.

For example, the following is an example specification for a rule for lumbar spondylosis:

Example rule specification:
Lumbar Spondylosis - Reasonable Hypthesis

Instrument: 62/2014
Factors: 6(d) ("lifting loads of at least 25 kilograms while bearing weight through the lumbar spine to a cumulative total of at least 120 000 kilograms within any ten year period before the clinical onset of lumbar spondylosis")
Satisfied:

1. The veteran has done at least 12 weeks of continuous full time service in the Army; and
2. The veteran has performed at least 10 days of operational service in last ten years.

Accumulation rate: 2413 kilograms per week.

4.1.3 Outputs

For set of Inputs as described above, the SoP Support Service has two outputs:

1. A machine-readable message containing the information necessary for other DVA computer systems to finalise processing:
    - A list of applicable SoP factors, identified by paragraph number and legislative instrument.
    - Denotation of which SoP factors are satisfied according to the processing rules set out above, if any.
2. A human readable 'case-summary' document in OpenXML document format (Microsoft Word 2007 and later) setting out:
    - The same information as in the machine-readable message above.
    - A summary of the input data, including:
        - The condition name and applicable SoP.
        - The date or date ranges of onset or aggravation of the condition.
        - A summary of service history in textual and graphical form.
    - For 'wear and tear' factors which include a threshold level of work and are not satisfied: the progress towards the threshold.

Following is an example excerpt of the machine-readable output for a case of lumbar spondylosis where the veteran has only peacetime service, but has nonetheless satisfied the requirements for at least one of the relevant factors according to the defined processing rules:

```
{
  // Note: this is the BoP SoP.
  "applicableInstrument": {
    "id": "F2014L00930",
    "number": "63/2004",
    "citation": "Statement of Principles concerning
    lumbar spondylosis No. 63 of 2014"
  },

  "factors": [
    // Factors 6(a) to 6(h) would appear here.
    {
      "paragraph": "6(l)",
      "text": "lifting loads of at least 35 kilograms while
       bearing weight through the lumbar spine to a
       total of at least 168 000 kilograms within any
```

```
      ten year period before the clinical onset of
      lumbar spondylosis, and where the clinical onset
      of lumbar spondylosis occurs within the 25 years
      following that period",
    "definedTerms": [],
    "satisfied": true
  }
  // Factors 6(j) to 6(o) would appear here.
  // Factors 6(p) to 6(ee) do not appear the case is
  // for clinical onset, and hence they are not relevant.
 ]
}
```

An example of the case summary document is at Appendix B.

4.2 SoP Reference Service

The Reference Data Service supports the following queries:

Query Description	**Query Parameters**	**Query Results**
Get SoP factors	1. Condition ICD code and name. 2. Standard of Proof (Balance of Probabilities or Reasonable Hypothesis). 3. Aggravation or onset.	A list of SoP factors from the **latest registered and in-effect** SoP for the condition from the Federal Register of Legislative Instruments, for the relevant standard of proof, filtered by aggravation or onset, including: • the legislative instrument number. • the legislative instrument citation. • a factor paragraph reference. • the full text of the factor and the full text of any definition for defined terms in the factor text.
Get Operations	Query Date	A list of warlike and non-warlike operations from the **latest authorised versions** of the Military Rehabilitation and Compensation (Warlike Service) Determination and Military Rehabilitation and Compensation (Non-warlike Service) Determination respectively, **which have commenced on or after the Query Date**, including the IDs of the latest versions of these instruments from the Federal Register of Legislative Instruments, and, for each operation: • The name of the operation. • The period.

For example, below as an excerpt of a response query to get SoP factors for the balance of probabilities standard, for aggravation, for lumbar spondylosis would return the following result:

```
{
  "registeredId": "F2014L00930",
  "instrumentNumber": "63/2004",
  "citation": "Statement of Principles concerning lumbar
       spondylosis No. 63 of 2014",
  "factors": [
    {
      "paragraph": "6(p)",
      "text": "having inflammatory joint disease in the
        lumbar spine before the clinical worsening of
        lumbar spondylosis",
      "definedTerms": [
        {
          "term": "inflammatory joint disease",
          "definition": "means rheumatoid arthritis,
           reactive arthritis, psoriatic arthropathy,
           ankylosing spondylitis, or arthritis
           associated with Crohn's disease or
           ulcerative colitis"
        }
      ]
    },
    //...
    //Factors 6(q) to 6(dd) would appear here.
    //...
    {
      "paragraph": "6(ee)",
      "text": "inability to obtain appropriate clinical
       management for lumbar spondylosis",
      "definedTerms": []
    }
  ]
}
```

Below is an excerpt of the response to a Get Operations query with a Query Date of 18 October 2016:

```
{

  "legislativeInstrumentIds": [
    "F2016L00994",
    "F2016L00995"
  ],

  "operations": [
    {
      "operationName": "Enduring Freedom-Afghanistan",
      "startDate": "2001-10-07Z",
      "type": "warlike"
    },
    {
      "operationName": "Slipper",
      "startDate": "2001-10-11Z",
      "endDate": "2009-07-30Z",
      "type": "warlike"
    },
    {
      "operationName": "Harwick",
      "startDate": "2014-07-21Z",
      "type": "non-warlike"
    },
    {
      "operationName": "Augury",
      "startDate": "2014-07-04Z",
      "type":  "non-warlike"
    }
    //... remaining operations would appear here.

  ]
}
```

4.3 Technical Requirements

The Services will be HTTP based web services with the following technical features:

1. Platform: Java Standard Edition 8 (Java SE8).
2. Application Server: Jetty.
3. Form of requests and responses:
    - JSON, REST style.
    - Accepts only GET requests.
    - API Key: none.
    - Authentication and authorisation: none (this is not necessary as the Components do not store any data requiring security protection).
    - Returns appropriate specific HTTP error and status codes out of: 200, 400, 401, 403, 404, 405, 429.
    - Dates in ISO 8601 format.
4. Processing:
    (a) Validates configuration on application start and logs errors.
    (b) Configurable throttling based on the number of requests from an IP address.
5. Security:
    (a) Secured against JSON and REGEX DOS attacks.
    (b) Secured against CSRF.
    (c) Configured for TLS 1.2 exclusively.
    (d) Validates incoming Content-Types and Response-Types.
    (e) Content-Type header includes charset.
    (f) Responses include header: X-Content-Type-Options: nosniff.
6. Server Configuration:
    (a) Cross Origin Resource Sharing enabled.
    (b) Gzip compression enabled.

7. Code Quality Metric: No ’Security’, ’Malicious code vulnerability’, or ’Multithreaded correctness’ warnings according to FindBugs 2.0.
8. Performance: average TTFB during up time over any 24 hour period of 500 milliseconds.
9. Deployment: The Services will be deployed to a PaaS cloud-hosting environment certified by the Australian Signals Directorate to “UNCLASSIFIED (DLM)” (which encompasses For Official Use Only and Sensitive: Personal markers).

5 Issues Discussion

5.1 Cloud hosting meets security requirements

The proposed cloud hosting of the Components meets security requirements under the Australian Signals Directorate's Information Security Manual[4] and the Defence Security Manual[5] for the reasons set out below.

5.1.1 SoP Reference Service

The SoP Reference Service is a mechanism to query publicly available data. It does not require, store or return any information other than publicly available information from the Federal Register of Legislation. Hence, it does not require any special security protections.

5.1.2 SoP Support Service

Host certified UNCLASSIFIED (DLM)

The SoP Support Service requires two sets of **anonymous** data as described above at section 4.1.1: condition data and service history data. The proposed cloud-hosted solution is certified by the Australian Signals Directorate to deal with data with a classification level of "UNCLASSIFIED (DLM)". This means the data must be Unclassified but may carry Dissemination Limiting Markers, such as "For Official Use Only" (FOUO) or "Sensitive: Personal". For the reasons set out below, this is **more than sufficient** to cover the data required. It is certified for one classification level **above** what is required. Further, other applicable mandatory controls in the Information Security Manual are also met for one level above what is required.

Personally identifiable service records UNCLASSIFIED (DLM)

The full, personally identifiable, service record of a veteran available to DVA is "Unclassified", with a Dissemination Limiting Marker of "For Official Use Only" under the Australian Government Security Classification System[6]. The sole marker which appears on the top of a full Defence ADO Service Record available to DVA via the SAM mechanism is "For Official Use Only". Similarly, the Data Management Agreement between DVA and Defence in relation

[4] http://www.asd.gov.au/infosec/ism/index.htm

[5] http://www.defence.gov.au/DSVS/defence-security-manual.asp

[6] https://www.protectivesecurity.gov.au/informationsecurity/Pages/AustralianGovernmentSecurityClassificationSystem.aspx

to PMKeyS data for the purpose of determining Qualifying Service states that "the data classification is considered For Official use Only (FOUO) as per existing information exchange"[7]. This marker may only be applied to unclassified information.[8]

Anonymous service records requires no DLM

However, this classification applies to the service record data when it is shown beside personally identifying details such as the name, address, and date of birth of the veteran. The service record data submitted to the SoP Support Service, on the other hand, will be anonymous. The test for whether the FOUO DLM applies under the Defence Security Manual is whether disclosure: "may cause limited damage to national security, Australian Government agencies, commercial entities or members of the public[9]". It is difficult to see how information that an an anonymous person participated in operations that are unclassified could would cause such damage. Hence, the service record data required by the SoP Reference Service does not even require the FOUO DLM. Hence, it does not require any special security protections.

Anonymous condition data requires no DLM

Similarly, the condition data is also anonymous. Submission of this data to the SoP Reference Service simply indicates that some unidentifiable applicant for DVA-administered benefits has the condition. This fact alone does not require special protection as there is no risk of harm from its disclosure.

To warrant a DLM, the condition data would have to be 're-identified' – i.e., linked to a particular person. If re-identified, it would likely amount to "sensitive information" under section 6 of the Privacy Act 1988 as it relates to "health information about an individual". Hence it would warrant the "Sensitive: Personal" DLM under the Defence Security Manual. The Office of the Australian Information Commissioner offers some guidance on the risk-assessment for re-identification.[10] This risk-based approach looks at the cost, difficulty, practicality and likelihood of re-identification.

Low re-identification risk

In this case, the risk of re-identification very low. To re-identify, a "motivated intruder" would have to match the condition data and accompanying service record data with some other source of information that identifies the individual.

[7] Page 8 of Defence-DVA Data Management Agreement, Version 1.0 (Final)

[8] Section 4.2.1 of Information security management guidelines, Australian Government security classification on system, Version 2.2; Paragraph 33 of Defence Security Manual, Part 2:30 published July 2015.

[9] Page 2 of Defence Security Manual, Part 2:30, published July 2015

[10] Privacy business resource 4: De-identification of data and information, accessed at https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-4-de-identification-of-data-and-information#assessing-the-risks-of-re-identification

However, there are no public or reasonably accessible sources of Defence service history data and medical records for veterans.

Secure even if re-identified

Finally, even if re-identification were practical, the maximum level of protection required would be for information with the DLM “Sensitive: Personal”. This is the level of protection Defence gives Sentinel incident reports, which similarly detail personally identifiable medical information. This is still within the UNCLASSIFIED (DLM) certification of the proposed cloud host.

5.1.3 ISM Controls

As discussed above, the information transmitted to the SoP Reference Service does not require any special security protections. Hence, the controls in the Information Security Manual do not apply. Nonetheless, this proposal still meets relevant mandatory controls for UNCLASSIFIED (DLM) material.

The relevant control relating to cloud hosting is “Control: 1395; Revision: 0; Updated: Apr-15; Agencies must only use outsourced cloud services listed on ASD’s Certified Cloud Services List (CCSL)”. This control will be met as the cloud host will come from this list: see above at 4.3.

The following are the relevant controls for securing information passing between DVA’s security domain and the cloud host:

Control	**How Met**
Control: 1447; Revision: 0; Updated: Apr-15: Agencies must use TLS (Transport Layer Security)	See above at 4.3.
Control: 0482; Revision: 4; Updated: Feb-14; Agencies must not use SSL.	See above at 4.3.
Control: 1373; Revision: 0; Updated: Feb-14; Agencies must not use anonymous DH.	The Components will be hosted on the Jetty application server, as set out above at 4.3. By default, this server does not enable any _DH_anon cipher suites.
Control: 1371; Revision: 0; Updated: Feb-14; If secure renegotiation is not available, agencies must disable renegotiation.	TLS is to be used exclusively: see above at 4.3.

Other relevant controls are also met:

- Personnel Security Control 0434; Revision: 4; Updated: Apr-15: met because all Gov Law Tech personnel have a current BASELINE or NV1 level security clearance on file with The Australian Government Security Vetting Agency (AGSVA).
- Control: 0445; Revision: 5; Updated: Apr-15: Agencies must restrict the use of privileged accounts. The only relevant privileged accounts are for administration access to the cloud-host provider's hosting environment. This is governed by the hosting provider's access policies. As set out above at at 4.3, the provider will be ASD certified to meet this control for UNCLASSIFIED (DLM) material.
- Event Logging and Auditing Controls are similarly met by virtue of the cloud-hosting provider's certification.
- Software Patching Controls are met by the strategy of using Platform as a Service functionality of the cloud-host. This will update automatically to the latest versions of the Java Virtual Machine and the Jetty application server, incorporating any security vulnerability patches.

5.1.4 Option of On-Premise Deployment

This proposal gives DVA the flexibility to deploy the Services on DVA/DHS infrastructure. DVA would be responsible for this. For the reasons set out above, we do not believe this is necessary for security reasons. Nonetheless, DVA may prefer this to cloud-hosting for production purposes as it gives DVA more control, albeit with an additional impost in time, cost and complexity.

If DVA wishes to go down this path, we recommended first to investigate more hands-on managed service offerings from the Whole of Government Cloud Services Panel as an intermediate step. These include access via a secure Gateway certified by the ASD to PROTECTED level. This still may be substantially more economical, faster and simpler than on-premise hosting.

The Services are not tied by design to cloud hosting or a particular cloud host. They are designed to run on the on the Java SE8 platform as standard HTTP based web services, and warranted to work correctly on the Jetty application server (see above at 4.3). This is a platform any party can set up on their own hardware without software licensing fees. It is a common platform used in cloud-hosted Platform as a Service offering from Microsoft and Google. For these reasons, its use is also consistent with the Digital Service Standard 7: "Use open standards and common platforms".

We are aware that DVA has successfully migrated such services from Jetty to its IBM Websphere Application Server instances on Windows Server 2003 during the MyService development process. We understand this is principally a server configuration and deployment task. In any case, the terms and conditions to this proposal allocate IP ownership in the code base to DVA. Hence, DVA is able to make any modifications necessary to suit its environment.

Regardless of DVA's ultimately chosen production platform, Gov Law Tech still needs to stand up the Services in an independently cloud-hosted environment. This is so Gov Law Tech can objectively verify the Services comply with this proposal. This is not possible using DVA's environment as Gov Law Tech cannot control its configuration.

5.2 SoP Reference Service Robust

Gov Law Tech's currently planned method[11] to ensure the SoP Reference Service automatically updates following new and amended SoPs is robust. Firstly, the method uses the only authoritative source for SoPs: the Federal Register of Legislation. The Federal Register of Legislation is established under the Legislation Act 2003 (Cth), maintained by the Office of Parliamentary Counsel at http://www.legislation.gov.au. Legislative Instruments (such as SoPs) are not enforceable unless registered on the Register in accordance with the Act. The Repatriation Medical Authority, as the rule-maker, is required to lodge SoPs with the Office of Parliamentary Counsel. This includes both new SoPs and amended SoPs. For amended SoPs, the RMA is required to lodge an up-to-date compilation. Hence, there is a legislative guarantee that this source is both authoritative and up-to-date.

Uses Federal Register of Legislation

Secondly, the method accesses the Register in a robust way. The method extracts required SoP information from the authorised PDF versions of SoPs. This is the only version that may be relied upon in court proceedings and contains a date of commencement. Each authorized version is identified by a unique official key which appears printed on the authorised version, known as the 'Register ID'. The Register serves up a web page at a particular URL which contains a link to download the authorised version. This is documented in the user guide for the Register.[12] Hence, there is no 'screen

No screen scraping

[11] NB: this section sets out currently planned implementation details of the SoP Reference Service, to give DVA assurance that the service will be robust. Gov Law Tech may vary the implementation at its discretion to meet its deliverables.

[12] See https://www.legislation.gov.au/Content/Linking

scraping' of SoP text. If the Register changes the way it displays SoP text on the screen, this should not impact the SoP Reference Service. The Register provides notifications of updates, including new, amended and revoked SoPs via a subscription. We have verified that this works and suits our purposes following the RMA's most recent round of changes to SoPs.

We have discussed the best method to retrieve authorised versions from the Register with the director of the publishing team at the Office of Parliamentary Counsel. We understand the method to be the simplest and most robust. The Australian Legal Information Institute[13] uses a similar approach.

Approach already used by others

In future, the way the Register provides information may change. However, this is unlikely to be without notice giving time to adjust – the Office of Parliamentary Counsel is aware of external computer programs that rely on the current methods. In fact, it is likely in future that the Register will become even more accommodating of robust programmatic access. It is a requested feature on data.gov.au and marked as "in review".[14] This following the lead of the United Kingdom and New Zealand, which already make regulations and legislation available directly to software applications via an Application Programming Interface.[15]

Finally, the structured, uniform nature of SoPs supports robust information extraction. Gov Law Tech prototyped and tested extraction from a variety of SoPs when scoping this proposal. SoPs issued since August 2015 follow a standard format. This format is fully documented in the "User Guide To the RMA Statement of Principles.[16] SoPs before this time follow a variety of formats. Gov Law Tech scoped and costed information extraction from these pre-August 2015 as part of this proposal.

5.3 Reliably Identifying Conditions

The Services require consuming applications to identify conditions by ICD code and/or condition name. This is different to our understanding of how DVA currently identifies conditions in its internal systems. Our understanding is that DVA has assigned a unique internal DVA code for each SoP. This code

[13] See http://www.austlii.edu.au

[14] See https://datagovau.ideascale.com/a/dtd/Commonwealth-Legislation-API/26897-26233

[15] See http://www.legislation.gov.uk/developer'
https://data.govt.nz/dataset/show/776
and https://regulationsgov.github.io/developers/

[16] See http://www.rma.gov.au/assets/FOI/PolicyuserguideAug15.pdf

is linked to a condition name and the instrument number defined by the RMA (such as “63/2014”). The DVA code is not necessarily connected to ICD codes in DVA’s existing systems or to a guaranteed up-to-date SoP.

ICD code is most robust ID

It is important to ensure DVA applies the correct the instrument to a given condition, as opposed to a repealed or subsequently amended instrument. Hence, there needs to be a durable way to link a condition to both current and future SoP versions. DVA’s current approach relies on constant manual updates to a table matching condition codes and names to SoP instrument numbers. This table becomes out of date whenever the RMA amends a SoP: the RMA uses a new instrument number for each amending instrument. It also becomes out of date if the RMA changes the name or phrase it uses for a condition, which is common. In these cases, DVA must manually update its reference data table. Otherwise, there ceases to be a reliable way to identify a condition exactly. Finally, the current system is vulnerable to minor spelling or punctuation errors in the often long and technical condition names.

The underlying design problem with DVA’s current approach is that it attempts to identify a medical condition by which legislative instruments refer to it, as opposed to features of the condition itself. However, there is already a more precise way to identify medical conditions which the RMA already uses: ICD codes. The most robust approach to identify the relevant SoP is to identify a condition by ICD code first. Then, given SoPs identify conditions by ICD code, we can find the correct and most up-to-date applicable SoP.

May ID condition by name also

Nonetheless, in many cases DVA it will be impractical for DVA to identify the ICD code for a condition. The Services also offer the option to identify a condition by its name, as a backup. When provided with a name and no ICD code, the Services will attempt to identify the relevant SoP by the condition name alone. For this to succeed the condition name must be exactly as it appears in the text of the SoP.