Senate Finance and Public Administration Reference Committee

ANSWERS TO QUESTIONS ON NOTICE

Supporting the development of sovereign capability in the Australian tech sector

6 May 2024

Department/Agency: Digital Transformation Agency
Topic: Retaining legacy data when implementing new systems
Asked by: Louise Pratt
Type of question: Hansard
Date set by the committee for the return of answer: 06 June 2024
Question on Notice Number: DTA-ISC-001

Number of pages: 3

Question:

Senator PRATT: How do you oversight the pockets of information that do clearly need to be pulled in from one methodology to another? I'm not a computer programmer; I don't know how variable the platforms are. When you're looking at trying to retain legacy data and you implement new systems that might do the same and/or new things, and you use that existing information in a new way or the same way, how do you see service providers' obligations for data exportability and the documenting of algorithms—or whatever, so that you can see what's being done to data—being carried over so that they can be transported from one provider to another?

Mr Poels: There are a few different issues there. To finish with the last piece, the DTA certainly does have visibility projects through the development stage. That's when projects are actively implementing a new system build. So we would have access to the ambitions and the technologies that agencies would be looking at: how they would deliver against the scope, whether data or a platform or a digital solution. We do lose a little bit of visibility once those projects become BAU, business as usual, and they move beyond the development stage into routine business as usual. What we are trying to do is make sure we strengthen up some of the requirements around what that information is being used for, how it's meeting user needs over time and, certainly in the AI space, whether it's fitting with the principles around effective use of AI. So there are a couple of different layers there: data, AI and everything else. But we do have, as I said, visibility in the active development stage, and we are increasingly trying to build our understanding of how agencies continue to use that technology to meet the needs of various users over time.

Senator PRATT: As an example, one of the companies this morning said, 'We could deliver PEMS for the ongoing running costs and develop a whole new system inside that budget.' How are agencies supposed to test that kind of proposition? How does an agency ensure that they haven't locked themselves into something they can't get out of because they'll never be able to get the data out of that?

Mr Poels: I might take the data question on notice. Certainly, in the case of PEMS and other technologies, from time to time they will become obsolete. They will run out of service and support, and at that point agencies may need to make a critical decision about what that next generation of technology and that next vendor might look like. That's when they might come back to government, for financial support to make that next investment. The DTA will be supporting them, to make sure that they're testing the market and that we understand the scale,

the scope and the intentions of what they are trying to seek money to invest in. We'll provide our best advice to government that they've actually done the due diligence, in terms of what they're looking to buy. Hopefully, some of the vendors might be useful in that space and provide those services.

Answer:

Data protection and portability is addressed in the Digital Transformation Agency's (DTA) sourcing contracts. For example:

- ***Privacy and Personal Information*** – DTA's agreements have clauses ensuring Seller's comply with all privacy Laws in respect of collection, use, storage, or disclosure of Personal Information (Hardware (clause 34), Software (clause 34), Cloud (clause 32), Telecommunications (clause, 33) Data Centres (clause 39), and Digital Sourcing Contract template (clause 12.1)
- ***Notifiable data breaches*** – DTA's agreements require the Seller to notify the buyer of eligible data breaches (Hardware (clause 35), Software (clause 35), Digital marketplace (clause 22), Data Centres (clause 39)
- ***Protecting Buyer Data and Material***:
    - Seller required to maintain any Buyer's data it holds securely and in accordance with Buyer requirements (Digital Sourcing Contract Template clause 12.3)
    - agreements include clauses requiring the seller to comply with directions and Buyer requirements relating to Buyer Material (Hardware (clause 69), Software (clause 69) Data Centres (clause 54).
- ***General security requirements*** - DTA's agreements include general security requirements requiring sellers to ensure Buyer Material (including data) is kept secure (Hardware (clause 66), Software (clause 66), Cloud (clause 29), Digital Marketplace (clause 15)), Digital Sourcing Contract Template (clause 12.5 and 13.2), Data Centres (clause 70), Telecommunications (clause 48).
- ***Cyber security*** – Sellers are required to take reasonable and prudent steps to reduce the risk of cyber attack (clause 13.3 digital sourcing contract template). DTA's agreements include security clauses relating to transmission of data (Cloud (clause 29)) Data Centres (clause 70), Telecommunications (clause 48)). Agreements set out Sellers are required to comply with PSPF and ISM.
- ***Transition out*** - DTA's agreements contain clauses that set out requirements for when a Contract ends to ensure the smooth transition from one supplier to another (Hardware (clause 65), Software (clause 65), Digital Marketplace (clause 23))
- ***Intellectual Property rights*** – DTA's agreements include clauses that set out when the Buyer owns/licences particular material under a Contract. This includes requirements that Intellectual Property created under the Contract held by the Seller or under its control is provided to the Buyer on expiration or termination of a Contract (Hardware (clause 49), Software (clause 49), Digital Marketplace (clause 8 Master Agreement and Clause 10 Comprehensive Terms), Data Centres (clause 37).

While clauses can help to avoid agencies from becoming ‘locked in’ with a particular vendor, there is a responsibility on agencies when it comes to planning their digital investments. Careful consideration must be given to how digital platforms are designed and integrated to enable information to pass between systems, and applying good practice and data standards enables migration (of data). This supports movement between vendors (and different digital solutions) and minimises the risk of data becoming stuck on obsolete technology. Agencies are encouraged to avoid a ‘monolithic’ architecture in the design of software which, once built, tends to result in programs which are more difficult to update and less adaptable to change (e.g., to accommodate emerging technologies).