Australian Government
Australian Taxation Office

UNCLASSIFIED External

Outcomes

Title:	Focus Group - Securing the broader ecosystem		
Issue date:	5 December 2018		
Venue:	WebEx		
Event date:	4 December 2018	**Start:** 12:00pm	**Finish:** 1:00pm

Chair:	Martin Mane	**Facilitator:**	Terry Seiver
Contact	Terry Seiver	**Contact phone:**	02 4923 1060

Attendees:	DSPs: Chris Howard – ABSIA/ADP Matthew Prouse – ABSIA/Xero Mike Behling - MYOB Keran McKenzie - MYOB Michael Wright - Sage Aaron O'Connor - Xero Michelle Lease - Intuit Simeon Duncan - Intuit Robert Fabian – Advance Payroll Rob Cameron - FYIdocs Daniel Wymer – ePayroll Mike Denniss – Class Super ATO: Martin Mane, Terry Seiver, Danielle Miller, Kylie Johnston
Apologies: **name/section**	Paul Murray – Account Kit Anne White - Ozedi

Next meeting	TBC

Agenda item: 1 – Welcome and Introduction

This group has been established in response to an action item from the SWG which called for a focus group to be established to understand the broader ecosystem and whether there is interest in developing commonly accepted standards across the industry.

The primary purpose of this group is to explore the interest in and development of commonly accepted security standards across the industry. The standards need to be developed by industry with the ATO’s role limited to helping to facilitate conversation.

DSPs recognised the value of bringing providers together to explore the issue further. Security standards should be consistent, verifiable but also support innovation.

The threats in the ecosystem are not just an ATO risk - all participants have ownership and responsibility.

Agenda item: 2 – Exploring the broader ecosystem

There was a general acknowledgement that the broader ecosystem refers to the third party application ecosystems, such as the ecosystems of accounting platforms.

As a starting point, the group discussed the aspects of the risk landscape which would need to be considered when developing common standards. These include;

- Sensitivity of the data
- Integration methods (eg flat file vs API call)
- Authentication and authorisation processes

Once the risk landscape has been established, the group can explore appropriate high level controls to mitigate or manage risks to an appropriate level.

The group acknowledged there was no single blueprint that could be utilised as a reference point. NIST may offer a basis for the risk based assessment process, however it was generally accepted that the NIST standard exceeded the likely risk profile.

Breach reporting should also be considered to ensure consistcy across the environment.

DSPs were keen to establish standards that were prescriptive but were vendor agnositic and allowed for flexibility in meeting the intended outcome.

Action item: 20181204_01	**Due date:** **Next meeting**	**Responsibility:** Focus group members

Group members will 'unpack' their environments:

- Risks
- Key data sets

Action item: 20181204_02	**Due date:** **Next meeting**	**Responsibility:** DPO

DPO to provide assurance of the point in the ecosystem at which the DSP Operational Framework ceases to apply, and the common industry standards being developed will take effect.

Agenda item: 3 – Success measures

The group agreed that success could be described as 'software developers are only required to meet the security standards once, in order to integrate with application ecosystems'

DSPs will need to consider what processes would be required to provide assurance against the standards. This may include auditing against a representative sample.

Agenda item: 4 – Next steps

The focus group will reconvene in the new year to un-pack the risk landscape and consider potential high level controls that may assist in the mitigation and management of these risks.

Action item: 20181204_03	**Due date:** **Next meeting**	**Responsibility:** DSPs

DSPs will provide details of software developers that produce third party add on products / services to the dpo@ato.gov.au for inclusion in this focus group

Action item: 20181204_04	**Due date:** **Next meeting**	**Responsibility:** DPO

The DPO will provide the draft DSP Operational Framework requirements for DSPs consuming DCL services.

Action item: 20181204_05	**Due date:** **Next meeting**	**Responsibility:** DPO
The DPO will reach out to Amazon and Microsoft to determine their level of interest in the outcomes of the focus group and the role they could play in raising awareness for their customers.		