Australian Government
Australian Taxation Office

UNCLASSIFIED External

Outcomes

Title:	Focus Group - Securing the broader ecosystem		
Issue date:	13 May 2019	**Venue:** WebEx	
Event date:	10 May 2019	**Start:** 11:00am	**Finish:** 12:00pm

Chair:	Terry Seiver	**Contact phone:**	02 4923 1060

Attendees:

David Field - Ozedi
Aaron Oconnor - Xero
Simeon Duncan – for Intuit
Michelle Lease - Intuit
David Martin - Intuit
Matthew Prouse - Xero
Simon Foster - Squirrel Street
Helen Macgillvray - Xero
Terry Seiver - ATO
Jason Phua - ATO
Roger Obbes - ATO
Danielle Miller - ATO

Apologies:

Chris Howard - ABSIA
Cristina Blumberg - ACCC
Michael Wright - Sage
Monica Winghart - Intuit
Phil Vella - Amazon
Anthony Migliardi - Xero
Daniel Wyner - Employ group
Jodi Ross - ACCC
Mike Behling - MYOB
Rob Cameron - FYI docs
Ann - Landmark Software
David Hawkins - Microsoft
Dino Alexandratos - Class
Karen Lay-brew - ABSIA
Lee Hickin - Microsoft
Selwyn Snell - Amazon

Next meeting	**TBC**

Key outcomes

Scope

Agreement reached around the definition of an ecosystem, '*internal and external API interfaces, which provide additional value add services to end customers*'. This involved the removal of the '*sold commercially*' component.

While a number of ecosystems exist, it was agreed that the focus would be on business, tax and accounting ecosystems.

Requirements

The Intuit security standards were seen as an ideal starting point.

The focus group agreed on the following high level requirements:

- Encryption key management
- Encryption in transit
- Multifactor authentication
- Indirect access to data
- App server configuration
- Vulnerability management
- Cookie management
- Encryption at rest
- Audit logging
- Data hosting
- Security monitoring practice

A number of requirements were excluded as they were not relevant or out of scope.

Considerations

Further to the requirements a number of issues need where discussed:

- The focus group agreed that the primary aim is consistency in the security standards. However there may be cases where either compensating controls could be utilised or the full set of requirements would not need to be met. For example where a requirement could not be met.
- Baseline assessment against the security requirements would be conducted by the ecosystem provider. However an independent assessment may not be relevant.

Next steps

DSPs with application ecosystems (as defined above) need to assess the specifics of each requirement and consider how they will affect their 3rd party add-on developers.

The focus group will need to agree to specific detail for each high level requirement.

DSPs also need to consider the specific thresholds for when the security requirements would apply to add-on developers e.g. number of customers or connections.

Actions

Action item:	Due date:	Responsibility:
20190511_1	Sunday 30 June 2019	DSPs
Review high level requirements outlined and provide feedback. Also assess the thresholds in which the requirements would apply to 3rd party developers.		

Action item:	Due date:	Responsibility:
20190511_2	Sunday 30 June 2019	ATO
Identify DSPs with ecosystems and distribute requirements for input and consideration		