Key Outcomes

Title:	Operational Framework Review – Supply Chain & Payload Encryption		
Issue date:	3 December 2020		
Venue:	WEBEX		
Event date:	17 November 2020	**Start:** 11:00am	**Finish:** 12:30pm

Chair:	Diana Porter	**Facilitator:**	Kylie Johnston
Contact	Diana Porter	**Contact phone:**	(02) 4724 0528

Attendees: names/section	ATO Kylie Johnston-Director Digital Partnership Office Miranda Shaw – Director, IT Security Paul Dwyer - Director, Digital Wholesale Integration Diana Porter - Digital Partnership Office Ian Lloyd - Digital Partnership Office Vitaly Sidorenko - Digital Wholesale Integration Bruce Cartland - DCIS Industry Chris Denney - SuperChoice David Field - Ozedi Holdings Grant Doherty - Qvalent Helena Bone - MessageXchange James Cameron - SuperChoice John Kennedy - Commonwealth Bank of Australia Mark Freestone - QSuper Matthew Prouse - Xero Michael Pogrebnoy - Automatic Data Processing Michelle Bower - Gateway Network Governance Body Rick Harvey - Layer Security Stephen Milburn - Sunsuper
Apologies: name/section	Toby Amodio - Director, IT Security Claire Miller - Director, Digital Communication & Identity Services Mark Macdowell - IT Architect, DCIS Architecture

	Andrew Strong - AMP Helen MacGillivray - Xero Roderick Schneider - Tanda Ross Daws - IRESS

Next meeting	TBA

The key outcomes for this meeting are best read with the supply chain & payload encryption focus group presentation.

Agenda item: 1 – Introduction & Overview

An overview and re-cap of the 2017 consultation session principles and outcomes relating to supply chain and encryption provided. Additionally an overview of external findings and DSP feedback included 2 opportunites to improve integrity of transactions through supply chain and payload encryption.

Agenda item: 2 – Supply Chain

Discussion on current compensating controls within the supply chain business solution.

Key points from industry discussion and feedback included:

- Clarification scope of interactions for this discussion, includes Business to Government interactions.
- Discussions to be taken offline in relation to e-invoicing and gateway interactions.
- External systems could have multiple layers or services before data is sent into the ATO, for example a roster management app which provides data to a payroll product for STP reporting.
- Threat modelling activities undertaken by ATO to identify risks within the supply chain.
- Requirement to be based on demonstrated risks as opposed to theoretical risks.
- Maturity of controls within the supply chain has improved over time through:
    - DSP Operational Framework implementation
    - Security Standards for Add-on Market places
    - APRA CPS 234
    - Supermatch terms and conditions version 9
- Overall number of client records breached with potential compromised identity has decreased since 2017.

Agenda item: 3 – Payload Encryption

Discussion on technical solutions and adoption methodology for payload encryption.

Key points from industry discussion and feedback included:

- Mixed sentiment from the group on whether payload encryption is or is not required.
- Group consensus, that if payload encryption is implemented it should be an optional requirement to support various business models whilst still protecting the ecosystem where required.
- Payload encryption to be implemented from the end user to the recipient.
- Clear definitions of who the end user is and at what point data becomes ‘tax or super data’ in scope of Operational Framework is required.
- Payload encryption to be assessed on a risk scale against the other models delivering data to the ATO.
- Further investigation regarding the SSP model is required to determine if it still works in our current environment and:
    - potential modification to support alternate authorisation models e.g. CAA
    - payload encryption to support extension of model to other services.
- Payload encryption to be assessed on a risk scale against the other models delivering data to the ATO.
- Less risk of security incidents if the ATO pulls data from the source rather than receiving data.

Agenda item: Wrap Up & Next Steps

Outcomes of the focus group to be published and circulated, members are encouraged to provide further feedback and comment.

ATO will establish a second meeting in December.