Australian Government
Australian Taxation Office

Key Outcomes

OFFICIAL External

Title:	Operational Security Framework (OSF) Review Combined Working Group Update		
Issue date:	30 June 2021		
Venue:	WEBEX		
Event date:	11 June 2021	**Start:** 13:00	**Finish:** 15:00

Chair:	Diana Porter	**Facilitator:**	Diana Porter
Contact:	Julie Huynh	**Contact phone:**	(02) 8894 9304

Intent:	Provide industry with an update on proposed outcomes of DSP OSF Review.

Attendees:

ATO	
Kylie	Director, Digital Partnership Office
Diana Porter	Operational Framework Lead
Fiona Homan	Direction, Information & Cyber Security
Anu Duggirala	Director, Digital Wholesale Integration
Toby Amodio	Assistant Commissioner, Information & Cyber Security
Simon Kert	Director, IT Security
Mark Macdowell	Director, DCIS
INDUSTRY	
Shaun Wilkinson	Ascender Pay
Craig Booth	Australian Business Software Industry Association
Paul Larsen	Australian Super Funds Association
Michael Pogrebnoy	BT Financial
Tim Covark	Class Super
Philip Boadi	Commonwealth Bank of Australia

Koustubh Bandyopadhyay	Commonwealth Bank of Australia
Michelle Bower	GovReports
Sandeep Gopalan	Iness
Ross Daws	Institute of Certified Bookkeepers
John Paul Lonie	Iress
Ross Daws	Iress
Rick Harvey	Link Administration Holdings
Matt Rea	MessageXchange
Mike Behling	MYOB Australia
Matthew O'Loughlin	Ozedi Holdings
Andrew Smith	Ozedi Holdings
Josef Bobinac	Ozedi Holdings
Mark Freestone	Qvalent
Grant Doherty	Reckon
Estevan Chaves	Sage Software Australia
Michael Wright	Sage Software Australia
Simon Foster	Sunsuper
Chris Denney	Superchoice
Stephen Milburn	Superchoice
Karl Farrand	Thomson Reuters
Mary Yeruva	Thomson Reuters
Helen MacGillivray	Xero
Matthew Prouse	Xero
Erin Adams	Xero
Jack Wee	Xero

Apologies:

ATO	
Melissa Goodwin	Director, DCIS
Claire Miller	Director, DCIS
Nick Kelly	IT Security Analyst DCIS Architecture
INDUSTRY	
David Delaney	Arrow Research Corporation
Shaun Wilkinson	Ascender Pay
Craig Booth	Australian Business Software Industry Association
Paul Larsen	Australian Super Funds Association
Michael Pogrebnoy	BT Financial
Kim Sung Do	Cashflow Manager
John Kennedy	Datacom Solutions
Doreen Bhamji	ELMO Software
Artur Czernecki	e-Payday
Brett Reed	Gateway Network Governance Body
Matthew Addison	Intuit

Simeon Duncan	Intuit
Matt Lewis	Iress
Andrea Cooper	Layer Security
Helena Bone	MYOB Australia
David Field	Paypac Payroll
Belinda Stewart	Pronto Software
Gary Semple	Qsuper
Simon Hutchinson	Sage Software Australia
Janice Aldinger	Storecove
James Cameron	SuperConcepts
Grant Christensen	TaxLab
Clyde Netto	Total Forms

Next meeting	TBA

The key outcomes for this meeting are best read in conjunction with the updated DSP Operational Security Framework Requirements and the Final Working Group presentation, paying particular attention to slides 11 & 12 (summary of changes) and 14 to 23 (detailed changes).

Agenda item 1: Introduction

DPO welcomed the combined working group members to provide an update on the outcomes and completion of the DSP OSF review.

The session covered:

1. Recommendations & Outcomes
2. Summary of Proposed Changes
3. Detail of Proposed Changes

Agenda item 2: Implementation

- It was noted that the PwC assessment identified 9 strengths, 17 recommendations and 6 areas of improvement. This led to the creation of 4 focus groups and 10 DSP consultation sessions with 50+ DSP/industry representatives.
- A brief overview of the DSP Operational Security Framework implementation timeline was provided highlighting key collaborations between industry and ATO since implementation.
- A few of the recommendations required internal ATO action only, which have been completed. Some recommendations required exploration through internal and external consultation and remain noted for potential future programs of work i.e. payload encryption.

- The remaining items were consulted with both industry and internal ATO SMEs. Which resulted in changes to the DSP OSF requirements and documentation, circulated to industry for feedback on 30 June 2021. The final documentation is expected to be finalised in July 2021.

DSPs implementing and meeting the new requirements will need to abide by the following:

- For all existing certified DSPs, implementation should be aligned to the next annual review cycle.

- If DSPs are unable to meet the changes by their next annual review date (based on the annual review occurring within 6 months of publishing), they are advised to contact the DPO to discuss their circumstances and implementation timeframes.
- For all new DSP OSF submissions, DSPs will need to meet the requirements from the date of publishing.

Outcome from industry discussion:

- Acknowledgement and agreement of the approach.
- DPO will work with DSPs who have any concerns in meeting the implementation timeframes.

Further consideration needed for:

- DPO will provide additional information including scenarios in a newly created support page within the knowledge hub of OS4DSPs to support adoption or application of the requirements.

Agenda item 3: Recommendations and Outcomes from the four focus groups

The group discussed outcomes from the four focus groups providing an opportunity for each group to hear a summation of what had been discussed and the outcomes achieved through consultation.

The outcomes from each focus group are summarised in the Final Working Group presentation on slides 5 to 9.

Key highlights of the outcomes include:

Authentication

a) Entity Validation
   - Entity validation is a new requirement in the DSP OSF. The minimum standard would be to verify that it is a valid business accessing your services. This can be done through the registration process, ensuring the contact details are legitimate.
   - Entity validation does not negate the need for DSPs to meet specific service requirements relating to verification e.g. SuperMatch requires specific customer verification requirements as part of the terms of use.

- There are conversations with DTA to work through using myGovID and RAM on a broader scale.

b) Multi-factor Authentication & Single Sign On
   - MFA has been uplifted to ensure any user accessing any data from within a DSP controlled/cloud environment will require mandatory MFA.
   - Social media cannot be used to login for MFA/SSO, however authenticator apps are allowed. DPO will ensure updated guidance.
   - Examples of authentication / single sign on will be provided in the knowledge hub.

Fraud Detection & Monitoring Focus Group

c) Audit Logging
   - Logs are to be kept for a minimum of 12 months. Shared logins not permitted.
   - More information will be available in the knowledge hub.

d) Reporting Security Incidents
   - Clarification on the word immediately, ATO has defined the term immediately as soon as practicable and should be within a few hours of an incident becoming known.
   - The intent for DSPs to report immediately is to enable remediation as soon as possible to mitigate the damage or threat to clients and systems. We understand that further investigation maybe required by the DSP and this information can be submitted when known.

Supply Chain & Payload Encryption

e) Supply chain & Payload Encryption
   - Payload Encryption was a recommendation, and whilst ideal, there are other higher competing priorities within the ATO, it will be explored in the future.

Requirements & Lifecycle Management

f) Certification
   - DPO will now accept self-certification of ISO 27002, ISO27017 and NIST as an additional standard to support DSPs.
   - NIST is acceptable for low/medium risk APIs, DSPs needing to undertake a maturity assessment.
   - When a DSP is required to uplift to independent certification, additional time may be provided. The DPO will work with the DSP to support transition timeframes.
   - The number of Taxation, Accounting, Payroll and Superannuation unique records will be checked for DSPs who are unsure of volumes.

Note: Product IDs are to be kept private and only used for the product it has been assigned to. The possibility of generating a test ID for developers will be reviewed.

Outcomes from industry discussion:

- Acknowledgement and agreement of the approach.

- Wording to be updated within the pack to clearly state and include the words social media. Further authentication solutions will be provided within the knowledge hub.

Further consideration needed for:

- DPO will provide additional information including scenarios in a newly created support page within the knowledge hub of OS4DSPs to support adoption or application of the requirements.

Agenda item 4: Summary of proposed changes

DPO provided a high-level overview and summary of proposed changes on slide 5 of the Final Working Group update presentation, these included 6 possible technical changes to implement or harden existing controls.

These can be found below:

Audit Logging

- Uplift: Timeframe included; logs must be kept for a minimum 12 months.

Certification

- Inclusion: ISO 27002, ISO27017 and NIST to support smaller DSPs in undertaking self-certification.

Data hosting

- No change to control, general improvements made to supporting guidance.

Encryption

- Clarity: Use of encryption protocol, all DSPs must use TLS 1.2 or higher.

Entity Validation:

- New requirement: Ensures the consumer/user of a commercial software product is a legitimate business and has a genuine need to access a DSPs software. The consumer/user must have a valid contact person with contact details, e.g. email and phone.

Multi-factor Authentication:

- Uplift: All cloud environments must have MFA in place to access any data in scope of the DSP OSF.
- Uplift: Remember me functionality limited to 24 hours.
- Uplift: Shared logins are not permitted and need to be blocked by the DSP.

Personnel Security

- Clarity: No significant change to the control, general improvements made to supporting guidance.

Security Monitoring

- Uplift: Control uplifted to include security monitoring for all DSP controlled environments.

Supply Chain & Payload Encryption

- Clarity: No change to control, general improvements made to supporting guidance.
- ATO not progressing payload encryption at this stage (remains a future work item).

OSF Process & Guidance

- Change of name to DSP Operational Security Framework.
- Inclusion to maintain the privacy and security of a DSPs unique product ID.
- Streamlined annual review procedures.
- Improved security incident reporting processes.
- Proposed knowledge hub content (Online Services for DSPs) to support understanding and completion of OSF.

Outcomes from industry discussion:

- Acknowledgement and agreement of the approach.
- DPO will provide additional guidance within the requirements documentation.

Further consideration needed for:

- DPO will provide additional information including scenarios in a newly created support page within the knowledge hub of OS4DSPs to support adoption or application of the requirements.

Agenda item 5: Detail of Proposed Changes

DPO provided a summary of slides 14 to 23 of the Final Working Group presentation, making it easier to review changes from existing to new documentation. This change log has been created as the existing documentation has been entirely restructured and reformatted into a streamlined document.

Overall outcome and next steps:

- Acknowledgement and agreement of the approach.
- Over the next 3 to 6 months DPO will progressively build out additional information. Including scenarios in a newly created support page within the knowledge hub of OS4DSPs to support adoption or application of the requirements.
- Outcomes of working group to be published and circulated.
- Once the document is published a further session will be scheduled to walk industry through key updates and changes.