Australian Government
The Treasury

DATA STANDARDS BODY

OFFICIAL

Data Standards Body

Information Security (InfoSec) Consultative Group

Background

In 2023, we saw threat actors compromise Australia's critical infrastructure and businesses at a scale and size not previously witnessed. Cyber threats remain a key risk in 2024 to Australian business and the safe and secure management of consumer data. As cyber threats continue to evolve at pace, the CDR must continue to improve its security, minimise risks and adapt to best protect consumers and their data. Improving cyber resilience in kind, requires changes to the Security Profile of the Data Standards. In addition to cyber threats, the other drivers of change to Data Standards generally include:

- Improved security for consumers and participants: remediating security gaps along with improving baseline security controls to provide a safe and secure environment for data sharing,
- Improved interoperability and open standards alignment: ensuring that the Data Standards maintain alignment to international standards for digital identity and authorisation, and minimise bespoke or proprietary security requirements,
- Reducing costs for implementation and maintenance: in turn this ensures changes to the Data Standards maintain vendor support limiting the need for costly customisation, and
- Improving consumer experiences: for example, modernising authentication standards to provide stronger customer authentication with safer and more intuitive authentication factors.

In 2023, the DSB consulted on authentication uplift. The DSB sees this as the first stage of uplift to the information security profile to improve security, modernise the Data Standards and enhance the consumer experience, whilst, at the same time reducing cost. Given the significance of this change and future planned changes, the DSB is seeking more engagement from cyber security experts in the next chapter of the Security Profile to input into and peer review the changes necessary to improve security whilst reducing costs (implementation, maintenance, compliance and risk) and improving the consumer experience.

To address the substantive change and the complexity of that change, the Chair is establishing a trial consultative group. The intent of this trial is to test an approach that provides a more targeted forum to progress cyber security matters with a membership that is representative of CDR participants which includes experts in cyber security.

If this trial demonstrates that the approach is effective, the DSB will propose that a more permanent version of the group be established

Terms of Reference

The InfoSec Consultative Group would be established by the Data Standards Chair as a group to provide advice to the Chair on the development of standards.

Under Section 56FA of the *Competition and Consumer Act 2020 (Cwlth),* the Data Standards Chair may make data standards. These data standards support the implementation of the Consumer Data Right (CDR).

Under Section 56FK, the function of the Data Standards Body (DSB) is to assist the Data Standards Chair (Chair). It must comply with the consumer data rules (enabled under *Competition and Consumer (Consumer Data Right) Rules 2020 (Cwlth)* when assisting the Chair.

Under Division 8.2 of the CDR Rules, the Data Standards Advisory Committee (DSAC) provides advice to the Data Standards Chair. The DSB provides support and secretarial services to the DSAC and the other committees, advisory panels or consultative groups the Chair may create.

The scope of the initial consultative group is proposed to be as follows:

- To define the required security elements to provide trust in the ecosystem and preserve the security of The Register, ADRs, Data Holders and consumers alike.
- To provide strategic guidance and input into the uplift required to the Information Security profile in the near term as well as considerations over the longer term that should be considered.
- To collaboratively work through significant security profile uplift towards a consensus position.
- To propose changes to the CDR Information Security profile that can then be commented on by all CDR participants in a public consultation.
- To provide feedback on the effectiveness of the trial and help shape a more permanent approach for the management of Information Security.

Membership

The membership of the initial Information Security Consultative Group will be determined as follows:

- Nominations will be open to anyone to become a consultative group member.
- Diversity in representation across Data Holders, Data Recipients, CDR and cyber security vendors, and international standards organisations involved in security is desirable.
- The preferred criteria for membership are:
    - Representative of an existing, operationally active, participant in the CDR ecosystem,
    - Technical expertise in the delivery and management of digital infrastructure,
    - Ability to work collaboratively in a group,

- Capacity for attendance at a regular monthly meeting, and
- Capacity to contribute time and personnel to review and comment on draft standards between meetings.

- The target size for the consultative group will be twelve members.
- Members will be required to accept a code of conduct that will include requirements for managing confidential or sensitive data provided to the consultative group to help with design and decision making.
- In addition to the members of the consultative group the ASD, ACCC, Treasury and OAIC will be invited to nominate an observer.
- The Data Standards Chair will have sole discretion on the number of members for the Information Security Consultative Group and the individuals that shall be invited as members or observers.
- Membership is made to named individual levels and membership may not be exchanged between individuals of one organisation without express agreement by the Data Standards Chair.

Whilst the standard cadence is anticipated to be monthly, it is expected that a fortnightly call will be necessary at inception due to the volume of work items in the backlog.

Operations

It is proposed that the consultative group will operate as outline below:

- The DSB will act as Chair and Secretary for the meeting.
- The consultative group will meet once per month for around one hour.
- An agenda, describing issues to be discussed will be published ahead of the scheduled meeting time.
- Available data, if any, that can be used as an aid to discussion will be made available to members ahead of the scheduled meeting time.
- Membership shall be made publicly available on the DSB website
- Minutes will be taken for each meeting documented the discussion and outcomes.
  - These minutes will be published publicly on the DSB website
  - The minutes will not contain attribution of anything said in the meeting or any sensitive information
- The agenda and minutes for each meeting will be considered public and will be published by the DSB.

- Meetings will be recorded for note taking purposes only. All recordings are kept securely as are the transcripts which may be made from them. No identifying material shall be provided without the participant's consent.
- The initial backlog of issues to address will be created by the DSB based on feedback received to date.
- This backlog will be maintained publicly on GitHub
- Once operational, the consultative group will actively curate the backlog of issues to address.
- The input of the Consultative Group will be captured and shared through a range of mechanisms to ensure it aligns with other workstreams across the DSB and CDR, including but not limited to:
    - Regular reporting into the Data Standards Advisory Committee on substantive progress and changes in information security. This may also include a request for feedback or direction from the DSAC.
    - Progression towards decision proposals once there is a pathway forward on key issues. This may also include experimental, or draft candidate standards.
    - Creation of change requests where changes are incremental.
    - Comments directly on existing change requests and Decision Proposals that are discussed in a consultative group meeting

Trial Conditions

Establishment of the consultative group will be sense checked periodically. An initial trial run of eight meetings will provide enough time to validate the operation of the consultative group, its effectiveness and ability to feedback into existing DSB operations for standards maintenance and decision proposal consultation.

If it is determined that the trial is not effective, it may be ended early. If the trial is considered successful it shall remain in establishment

For further information

Mark Verstege
DSB Technical Lead
mark.verstege@@consumerdatastandards.gov.au

Michael Palmyre
DSB CX Lead
Michael.palmyre@consumerdatastandards.gov.au

Terri McLachlan
DSB Secretariat
terri.mclachlan@consumerdatastandards.gov.au