Voluntary Data Classification Framework

The voluntary data classification framework (the framework) will assist Australian industry organisations to classify and define the value of their data in a consistent and unified way. CSIRO's Data61 is working in partnership with Department of Home Affairs (Home Affairs) to develop the framework, which will be available by late 2025. The framework is a commitment outlined in the _2023-2030 Australian Cyber Security Strategy_.

Why develop a framework?

- Effective cyber security is underpinned by an organisation's understanding of the nature of data being held, the risks associated with that data, and its value[1].

- The Australian Government recognises that industry is best placed to consider the value of their data. At present, there is no standardised system to assist the private sector to classify the data they hold.

- Home Affairs has received consistent feedback from industry on the need for a voluntary data classification framework.

Aim of the framework

- The framework will guide industry to identify, assess, classify and communicate the value of their data holdings in a consistent way.

- This will enable businesses to segment information and implement proportionate operational controls to reduce enterprise risk.

- It will be practical to use and interoperable with existing classification systems, including the _Protective Security Policy Framework_ (PSPF) which applies to Australian Government entities.

How is the framework being developed?

- It will be informed by research undertaken by CSIRO's Data61 on the broader data risk management landscape.

- The framework will be based on information and feedback collected through consultation with industry and Commonwealth agencies.

- The consultation process will engage with businesses, peak bodies and other organisations covering large and medium enterprise, family or sole traders, and start-ups. Representation will be from across a range of different industries and sectors.

- It will be piloted with a small group of industry representatives. Findings from the pilot will be used to inform the framework.

Benefit of the framework

There are several anticipated benefits to having a consistent data classification framework for industry, including:

- ✓ **uplifting** security controls to be applied to data, proportionate to the value, importance and sensitivity of the data
- ✓ **empowering** industry to strengthen their cyber security posture and support secure data practices
- ✓ **strengthening** data governance approaches to reduce barriers and build consumer trust when sharing data
- ✓ **enhancing** the consistency of data management, including how data is stored and shared
- ✓ **unifying** the classification of data based on its level of sensitivity, value and criticality to an entity.

How do I find out more?

- Visit the Home Affairs website[2] or the CSIRO project website[3] for further information.

If you would like to be considered for the consultation process, please email us at DataClassification@csiro.au.

---

[1] By value, we mean the cost of collecting the data, the value or worth to the business, and the costs if it were to be stolen, leaked or lost.

[2] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/technology-and-data-security/voluntary-data-classification-framework

[3] https://research.csiro.au/dataclassification