National Data Security Action Plan

24 June 2022

Science & Technology Australia thanks the Department of Home Affairs for the opportunity to offer feedback on the National Data Security Action Plan discussion paper. STA is the peak body representing more than 90,000 scientists and technologists in Australia.

Data definitions in the STEM and research sector

Research data

Data underpins virtually every facet of research endeavour, and is derived from a vast array of sources. It encompasses physical, chemical and biological information about environmental, animal and human systems, as well as social and population-level information. Scientific data is not only stored in a digital format – it can include physical samples, such as specimens in museum and herbaria collections, as well as visual imagery and acoustic recordings.

Research data of all forms and types is collected, stored, analysed and shared continually as research projects progress. Individual researchers and research teams are responsible for their own data and must be able to access, analyse and share it according to the project needs. Any data security guidance must account for the incredibly disparate nature of research data and the variety of researchers, research teams and institutions that work with datasets.

Some research data is derived from people, and as such is sensitive and already subject to significant regulatory requirements. Sensitive or personal data held by government organisations for research is nearly always de-identified before researchers can use it, and is already subject to significant regulatory requirements. In Australia, strong ethics approvals protections are in place for human research, with institutional ethics committees carefully assessing sensitive issues before issuing ethics approvals for research projects. Additional layers of compliance to access or use this type of data would be unnecessary.

The Australian Code for the Responsible Conduct of Research, developed by the Australian Research Council, the National Health and Medical Research Council and Universities Australia, contains a section on data use and management. This provides comprehensive guidance to researchers and research institutions on how research data, as well as sensitive or confidential data, should be managed. Research grant funding contracts often also include specific requirements on project data management. For example, some Commonwealth Government funded grants require all data and publications to be made open access.

Institutional data

As well as research-generated data, universities and research institutes maintain databases with significant personal data related to staff and students. Ensuring this data remains secure is imperative, and Australian universities are continuously strengthening their cyber security protocols and acting on advice from key national agencies.

Providing a framework of data security standards may help improve consistency across the sector, but given the significant investments institutions already make in data systems and storage, such standards should be issued as a guide rather than a further mandatory compliance obligation.

Current regulations on the sector

Universities and research institutions have faced a significantly heightened regulatory environment in recent years, navigating a vast array of legislation on national security, foreign interference and cyber security.

These include:

- the Australian Code for Responsible Conduct of Research
- the *Defence Trade Controls Act 2012* and the Defence and Strategic Goods List;
- the Sanctions Regime;
- the Blueprint for Critical Technologies;
- the University Foreign Interference Taskforce Guidelines to Counter Foreign Interference in the University Sector;
- the *Australia's Foreign Relations (State and Territory Arrangements) Act 2020*;
- the *Foreign Influence Transparency Scheme Act 2018*;
- the *Security Legislation Amendment (Critical Infrastructure) Act 2021* and *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*

Universities and researchers take security concerns very seriously and understand the importance of a robust approach to national security and data integrity. Over-regulation and overlapping or duplicative legislation designed with a 'catch-all' approach risks curtailing research collaborations as well as industry investment and development. Australia's STEM sector must be supported – and protected – by developing collaborative and targeted risk-based solutions.

The existing compliance burden is significant, and every dollar that is spent on meeting regulatory requirements is a dollar not spent on supporting research. A voluntary framework that would guide institutions' approach to data security would be vastly preferable to another layer of regulation.

A recommended approach would be to provide support for universities, research institutions and businesses to access advice and guidance on best practice for data security. A dedicated team in the Department of Home Affairs, along the lines of the support historically provided by the Department of Defence to assist universities navigate the Defence and Strategic Goods list, would be an excellent model to follow. Positive support and assistance, rather than compliance penalties, would greatly assist Australia's research sector to adopt any new protocols with maximum effectiveness.

International collaboration and data sharing

Science depends on the free flow of information between global collaborators. The most significant challenges facing society will only be solved through concerted global efforts, and these collaborations must be supported, not hindered, through restrictions on data sharing or storage. Australian researchers must be able to collaborate with international partners, and this will require data protocols compatible with international guidelines, but also the ability to share and potentially store data using systems that will potentially be located overseas.

Additionally, the growth of distributed data storage schemes using systems like blockchain makes the actual location of data storage 'borderless'. Any data security framework and future policies must recognise this and be able to accommodate the rapidly evolving product and best practice market.

Open data

Open data has the potential to greatly advance progress within the research sector – the open sharing of COVID-19 data globally led to rapid breakthroughs in vaccine development, at an unprecedented pace.

Ensuring data is secure is of paramount importance, but this must be done in a proportionate and reasonable manner that still enables the sharing and openness essential to progress research.

Similarly, data security must not be used as a means to prevent transparency and data accessibility. There are significant datasets collected by various levels of government that can provide useful insights to researchers – these datasets should be made open and accessible to researchers, with appropriate guidelines for use.

Indigenous data

Any data security protocols must also engage strongly with the issues of ownership, security, uses and informed consent protocols related to Indigenous data. Indigenous data and knowledge is subject to cultural considerations and specific perspectives on how this data can be used or shared, where and how it should be stored, and who can access it. Indigenous researchers and research organisations must be consulted to seek their views on how a national data security strategy should incorporate these considerations.

Consultation paper questions

Responses to the specific consultation paper questions pertinent to the university and research sectors are provided below.

1. What do you consider are some of the international barriers to data security uplift?

Different levels of awareness and data security capabilities across different countries contribute to international data security challenges.

2. How can Australian Government guidance best align with international data protection and security frameworks? Are there any existing frameworks that you think would be applicable to Australia's practices (e.g. the European Union's General Data Protection Regulation)?

The Australian Government should certainly look to international best practice in data security and management, and aim to provide a consistent approach that will best enable global research collaboration and data sharing.

3. What additional guidance or support from Government would assist you to meet a principles-informed approach to data security? How would this be delivered best to you?

Establishing a voluntary framework or set of recommended standards would be the ideal approach. Additional mandatory regulation would add to the already significant compliance burden upon universities and research institutes. The Department of Home Affairs could establish a dedicated team that universities, research institutes or businesses could call upon for advice and assistance in implementing best practice.

The ever-changing and increasingly complex cyber and data security landscape requires a trained skilled workforce equipped with the expertise to meet current and future challenges. The education and training sector should be supported to deliver new bespoke data security training programs and micro-credentials that allow professionals, scientists and technologists 'working at the coal face' to be skilled and up-to-date in these areas.

4. How could Australian legislative and policy measures relating to data security be streamlined to better align with your obligations in international jurisdictions? Does variation in international approaches create hurdles to your effective participation in the global market? a. What obligations are you most commonly subjected to from international jurisdictions?

A thorough analysis of all existing legislation and regulation universities must navigate (as outlined above) should be conducted to avoid unnecessary duplication, and a cohesive whole-of-government approach.

5. Does Australia need an explicit approach to data localisation?

The research sector is underpinned by global collaborations and scientific progress depends upon the free flow of data and information across international borders. Any data localisation requirements must acknowledge this, and not curtail research efforts.

Additionally, the growth of distributed data storage schemes using systems like blockchain makes the actual location of data storage 'borderless'. Any data security framework and future policies must recognise this and be able to accommodate the rapidly evolving product and best practice market

6. How can data security policy be better harmonised across all jurisdictions? What are the key differences between jurisdictions that would impact the ability to implement standardised policies/are there any areas of policy that could not be standardised? If yes, why?

Researchers often use data held by the federal and state governments, which already have restrictions on access and use. Additional protocols must not make this data even harder to access.

8. What are the main challenges currently faced by industry as a result of inconsistent data security practices between all levels of Government, including municipal governments?

Inconsistent and complex protocols that impede access to data or data sharing can lead to waste and be a significant drain upon time and resources within the research sector. Time and money that is spent meeting compliance requirements are resources not spent upon furthering Australia's research efforts.

9. What steps could your business take to better understand the value of the data they process and store? Do businesses have sufficient awareness of their data security obligations?

Universities and research institutes take data security concerns very seriously and are continually improving the sophistication of their approaches to data management and security. Universities all have IT infrastructure and data security teams. Extra layers of security are included as required for defence and sensitive research. They regularly get briefings from the ASIO and related agencies on data risk, upgrade cyber security infrastructure, and engage closely with the Government to respond to any incidents.

10. How can the Australian Government further support your business to understand the value of data and uplift your data security posture?

The Government should consider establishing a dedicated team to provide advice and support to organisations seeking to improve their data security measures. Access to dedicated skills would be particularly beneficial to smaller organisations or those who do not have the inbuilt high-level capacity or expertise in data management.

12. Should there be overarching guidance on securing data for businesses of all sizes, or is it important to provide guidance based on a company's size? For example, a 'size' threshold).

In the research sector, it will need to be acknowledged that there is a vast array of data being collected, stored and analysed continually. Individual researchers and research teams are responsible for their own data collection and storage – data security guidance must account for the incredibly disparate nature of research data and the variety of researchers, research teams and institutions that work with datasets.

13. Are there any limiting factors that would prevent Australian industry and businesses from effectively implementing an enhanced data security regime?

Universities and research institutes already navigate heavy compliance burdens that impose significant financial and personnel costs. Some research institutes are very small operations, and would struggle to meet additional resourcing costs that additional compliance would incur. Within larger institutions, costs are already significant, and having to divert more resources to additional compliance ultimately means there is less support for research efforts.

14. Does the Australian Government currently have sufficient public information for consumers and citizens on data security best practice? How can we make that information more easily accessible, usable and understandable?

A dedicated team that could provide support to organisations seeking to improve their systems would be beneficial.

It will also be beneficial for service providers offering consumer and industry level data services to be able to benchmark against consistent government standards. This will provide consistent levels of service and reassurance to customers.

15. Should there be enhanced accountability mechanisms for government agencies and industry in the event of data breaches? How else could governments and industry improve public trust?

Government should be the paradigm of data security and best practice, as well as data openness and best practice.

Please do not hesitate to contact us if we can assist with any additional information.

Professor Mark Hutchinson
President, Science & Technology Australia

Misha Schubert
CEO, Science & Technology Australia