Final report

Real-time, data-driven approach to assessing networked biosecurity risk

Project code: MLA V.RDA.2102

Prepared by: ExoFlare

Date published: 26 April 2022

PUBLISHED BY

Meat & Livestock Australia Limited

PO Box 1961

NORTH SYDNEY NSW 2059

Meat & Livestock Australia acknowledges the matching funds provided by the Australian Government to support the research and development detailed in this publication.

Abstract

The red meat and livestock industry has a total turnover of $69.9 billion including $33.7 billion in production and directly employs almost 196,000 people in the year 2019-2020 *(MLA, 2020)*. ExoFlare has employed a data-driven approach to biosecurity to support Australian agriculture in rapidly identifying and responding to biosecurity risks by providing access to real-time network risk assessment.

The end goal is to apply ExoFlare's novel biosecurity data platform to predict and respond to emerging risks relating to Australia's beef and sheep industry supply chains.

This project builds on V.RDA.2021 where beef and sheep meat data was prepared for inclusion in the Cross-sector Operational Biosecurity Risk Assessment (COBRA) platform in preparation for next phase analytics on key biosecurity risk vectors. Additionally, ExoFlare has received a Traceability grant from the Department of Agriculture, Water and the Environment (DAWE) to develop a real-time data-driven approach to assessing biosecurity risks in the red meat and pork sectors. Collaborating with industry leaders Meat & Livestock Australia (MLA) / Integrity Systems Company (ISC), Australian Pork Limited (APL) and SunPork Group, ExoFlare will develop a real-time, data-driven approach to assessing networked biosecurity risk.

Data sharing is the key requirement to enable such a biosecurity data platform and provide timely and useful information on potential risks to the members of the red meat industry throughout the supply chain. Our goal in this project is to explore how biosecurity data is currently shared throughout the Australian biosecurity system discover the perceptions of the value in data sharing, identify barriers that make data difficult to share, and find enablers that could overcome these barriers.

ISC contributed funding to this broader project to determine barriers and opportunities for data sharing between government and industry to inform the COBRA data integration project plan.

DAWE Traceability grant objectives (three year contract):

1. Detailed recommendations on linking digital traceability through supply chains with quantifiable biosecurity improvements to uphold the disease-free status of Australian pork and red meat
2. Demonstrated reduction of biosecurity risk through enabling traceable behaviour change to improve outcomes
3. Validated methods for comprehensive data capture and notifications to support rapid response to biosecurity outbreaks

Executive summary

Background

The red meat and livestock industry has a total turnover of $69.9 billion including $33.7 billion in production and directly employs almost 196,000 people in the year 2019-2020 *(MLA, 2020)*. ExoFlare has employed a data-driven approach to biosecurity to support Australian agriculture in rapidly identifying and responding to biosecurity risks by providing access to real-time network risk assessment.

ExoFlare's platform supports traceability and dynamic assessment of biosecurity risks across supply chains, including importation, production, processing and distribution. The end goal is to apply ExoFlare's novel biosecurity data platform to predict and respond to emerging risks relating to Australia's beef and sheep industry supply chains.

Objectives

ExoFlare was awarded a Traceability Grant for the Cross-sector Operational Biosecurity Risk Assessment (COBRA) project to develop a real-time data driven approach to assessing biosecurity risks in the red meat and pork sectors. The objectives of the COBRA biosecurity traceability program over three years are as follows:

1. Determine key risks and opportunities for data sharing between government and commercial organisations;
2. Validate methods to capture data and provide notifications on biosecurity risks;
3. Recommendations on linking digital traceability and biosecurity risks;
4. Demonstrate risk communications and behavioural changes to improve biosecurity.

This larger project was planned into three phases. The first phase aimed to understand how biosecurity data from across government and industry can be shared and analysed in new ways to improve our ability to manage existing risks and detect emerging risks sooner. This involved interviewing custodians of biosecurity data and other stakeholders to collect feedback and identify data sharing opportunities to determine the key risks and opportunities for data sharing between government and commercial organisations.

The first phase objectives, as covered in this report, are as follows:

1. Conduct red meat data custodian interviews with a minimum of 15 experts, document and summarise findings for provision to MLA;
2. Presentation of results and workshop with MLA on data sharing priorities.

Methodology

ExoFlare conducted 22 interviews including the Chief Veterinary Officers (CVO's) and key biosecurity officials of 5 states, key officials in 7 branches of DAWE, and 4 other industry organisations. These contacts are considered custodians and stakeholders for the data relevant to managing biosecurity risk in the red meat and pork sector. In these interviews, ExoFlare presented a general overview of a future biosecurity traceability system to get feedback on data available to support such a system and barriers and issues if such a system were developed.

Results/key findings

Through the workshops, ExoFlare validated the proposed COBRA biosecurity traceability system. There was a general agreement on the importance of data sharing, and the potential that could be

realised for industry if data that was collected on biosecurity risks were made available to the supply chain. However, barriers and risks to the sharing of the data currently prevent this from occurring.

In particular, ExoFlare identified four key data sharing risks raised in the interviews. Barriers to data sharing that were identified include the following:

1. Data is difficult to find or collate due to fragmentation of data across organisations and divisions;
2. The data sharing process is complicated, legally intensive, and time-consuming;
3. If shared, data is often not current or too coarse to be useful due to aggregation and lengthy data access processes;
4. Data sharing remains technically challenging, due to the prevalence of older systems that are not developed with data sharing front of mind.

Enablers to improve data sharing were identified based on previous programs to improve government-industry data exchange. These include the following:

1. Simplify data sharing negotiation process;
2. Move to online processes for permissioned data sharing sign-off;
3. Use tools to manage the risk of re-identification;
4. Standardise data collected for biosecurity management projects;
5. Leverage existing data-sharing frameworks;
6. Develop interoperability through APIs and long-term permissioned data access.

These enablers are described with reference to previous projects that have developed tools or processes that advance these areas.

Future research and recommendations

The next phase of the COBRA project will involve researching risk communications and behaviour change to provide those best placed on the ground with the information they need to respond to potential risks. In the final phase, a pilot experiment will be conducted to demonstrate risk communication and measure behaviour changes through the ExoFlare platform.

To realise the proposed COBRA biosecurity traceability system, the following next steps are recommended:

- Federal, state, and territory governments should pursue improvements in data sharing by following the recommendations of the National Agricultural Statistics Review *(ABS, 2015)* and the suggestions in the second Agricultural Statistics Roundtable *(ABARES, 2018)*.
- Industry bodies should continue with projects to enable permissioned exchange of agricultural data such as the Australian AgriFood Data Exchange project, to enable management of biosecurity by the supply chain.
- Use existing solutions for data release risk management and permissioned data access to improve data sharing within federal government departments, and between federal and state governments.
- Pursue further research into connecting risk information through the supply chain to enable a real-time, data-driven approach to assess networked biosecurity risk for the red-meat industry.

- Establish standardised protocols for digital biosecurity traceability data to state and territory government biosecurity offices. Such information includes digital records of visitors to the site that can be used for traceforward and traceback during emergency animal disease (EAD) events.
- Establish an open-data platform to collate real-time aggregated biosecurity risk information derived from government and private data.

Table of contents

1. Background

1.1 ExoFlare data-driven risk assessment

The red meat and livestock industry has a total turnover of $69.9 billion including $33.7 billion in production and directly employs almost 196,000 people in the year 2019-2020 *(MLA, 2020)*. ExoFlare has employed a data-driven approach to biosecurity to support Australian agriculture in rapidly identifying and responding to biosecurity risks by providing access to real-time network risk assessment.

ExoFlare's platform supports traceability and dynamic assessment of biosecurity risks across supply chains, including importation, production, processing and distribution. The end goal is to apply ExoFlare's novel biosecurity data platform to predict and respond to emerging risks relating to Australia's beef and sheep industry supply chains.

This project builds on V.RDA.2021 where beef and sheep meat data was prepared for inclusion in the Cross-sector Operational Biosecurity Risk Assessment (COBRA) platform in preparation for next phase analytics on key biosecurity risk vectors. Additionally, ExoFlare has received a Traceability grant from the Department of Agriculture, Water and the Environment (DAWE) to develop a real-time data-driven approach to assessing biosecurity risks in the red meat and pork sectors. Collaborating with industry leaders Meat & Livestock Australia (MLA) / Integrity Systems Company (ISC), Australian Pork Limited (APL) and SunPork Group, ExoFlare will develop a real-time, data-driven approach to assessing networked biosecurity risk.

1.2 Data Sharing

Data sharing is the critical requirement to enable a biosecurity data platform, and provide timely and valuable information on potential risks to the stakeholders of the red meat industry throughout the supply chain. Exoflare's project aims to explore how biosecurity data is currently shared throughout the Australian biosecurity system; discover the perceptions of the value in data sharing; identify barriers that make data challenging to share; and find enablers that could overcome these barriers.

Digitisation and data sharing underpin the first steps to a transformational trajectory for Australian agriculture to be considered the most bio-secure trade partner globally by CSIRO. The recommendations point to enhanced data sharing networks which can drive national coordination of biosecurity activities, and investments in new technology applications that can result in a system that more efficiently identifies and manages existing and emerging risks *(CSIRO, 2020)*.

The benefits of data sharing and open data have been widely recognised in government and academia *(AGPC, 2017) (Salsa Digital, 2022)*. Over the last decade there has been a move to open data, in 2015 the federal governments released the Public Data Policy Statement including the requirement of departments to share non-sensitive publicly as a default (DPMC, 2015). This was followed by the establishment of open data portals that catalogue and make available open datasets including data.gov.au and similar state and territory open data portals.

While the availability of open data has progressed significantly, the sharing of data that contains sensitive information is still a complicated and difficult process.

1.3 Previous data sharing recommendations

There is a wealth of previous literature on data sharing from both Australia and overseas and this report does not attempt to cover all previous work comprehensively. In this section selected key

reports are outlined which contain guidelines and recommendations for data sharing from academic, government, and industry perspectives.

In particular, the selected reports are relevant to agricultural data sharing between industry and government and do not cover all legislation that impacts data sharing, or the legal considerations and technicalities of releasing a particular dataset. These are categorised by the three main perspectives of academic, industry, and federal government.

Australian Farm Data Code

This is a voluntary code of practice that was designed by the National Farmers Foundation to apply to digital service providers which collect, interpret or manage data through a direct commercial relationship with a farmer *(NFF, 2020)*.

The code defines and covers three distinct categories of data

- Farm Data: data that originates from a farmer, or a service provider in the course of providing a service to a farmer;
- Private Data: data that could be used to identify an individual farmer or farm business; and
- Public Data: data from any source which relates to a farmer or their business not in the first two categories.

The Farm Data Code is governed by the following principles that must be adhered to by the service provider. These are best practices that have been developed with reference to similar voluntary codes of practice overseas including in the United Kingdom and New Zealand with the goal to improve the trust between the farmer providing the data and the digital service provider.

The seven principles as follows:

1. Transparent, clear and honest collection, use and sharing of farm data
2. Fair and equitable use of farm data
3. Ability to control and access Farm Data
4. Documentation and Record Keeping
5. Portability of Farm Data
6. Keeping Farm Data Secure
7. Compliance with National and International Laws

This code is of most relevance to the collection and use of data by digital service companies and affects how this data can be shared with government authorities even when this sharing is well-intentioned; for example, to improve biosecurity for Australia.

FAIR Data Principles

The "FAIR Guiding Principles for scientific data management and stewardship" were published as international principles to improve the Findability, Accessibility, Interoperability, and Reuse (FAIR) of digital assets (Wilkinson, 2016). These principles have been adopted by Australia's research community led by the Council of Australian University Librarians who chair the FAIR Steering Group (https://www.fair-access.net.au/about/steering-group).

The four main principles are as follows (ARDC, 2016):

- Findable: This includes assigning a persistent identifier, having rich metadata to describe the data and making sure it is findable through disciplinary local or international discovery portals.
- Accessible: This may include making the data open using a standardised protocol. However, the data does not necessarily have to be open (such as sensitive data). When it's not able to

be open, there should be clarity and transparency around the conditions governing access and reuse.

- Interoperable: This involves using community accepted languages, formats and vocabularies in the data and metadata.
- Reusable: Reusable data should maintain its initial richness. For example, it should not be diminished for the purpose of explaining the findings in one particular publication. It needs a clear machine readable licence and provenance information on how the data was formed. It should also have discipline-specific data and metadata standards to give it rich contextual information that will allow reuse.

Government Data Sharing

The Five Safes framework for the principled management of data disclosure risks was developed by the Office of National Statistics (UK). This framework has been adopted by the Australian Bureau of Statistics and the Australian Department of Social Service. In 2017 the Australian Productivity Commission recommended adopting a version of the framework to support cross-government data sharing and re-use (AGPC, 2017).

Each safe refers to an independent but related aspect of disclosure risk. The framework poses specific questions to help assess and describe each risk aspect (or safe) in a qualitative way. The degree to which each safe is controlled is used to assess the risk of disclosure (ABS, 2021).

The five elements of the framework are:

- Safe people: Is the researcher appropriately authorised to access and use the data?
- Safe projects: Is the data to be used for an appropriate purpose?
- Safe settings: Does the access environment prevent unauthorised use?
- Safe data: Has appropriate and sufficient protection been applied to the data?
- Safe outputs: Are the statistical results non-disclosive?

This is a key framework used by the government to risk-assess data sharing requests; however, it is not a legal framework and is not a replacement for the legal protections conferred under the privacy law. It is referred to as the recommended framework to manage the risks of data sharing in the Data Availability and Transparency Act 2022.

Data Availability and Transparency Legislation

The Data Availability and Transparency Act 2022 establishes a new, best practice scheme for sharing Australian Government data, underpinned by strong safeguards and simplified, efficient processes (ONDC, 2022).

The bill addresses key recommendations of the Productivity Commission's Inquiry Report into Data Availability and Use (PC, 2017) which identified a number of benefits of greater data availability and use including improving the integrity of systems and increase administrative efficiency.

In taking advantage of greater use of data, it is important to give appropriate attention to other interests such as privacy, security and intellectual property.

The Bill authorises Australian Government bodies to share government data with accredited users for specific purposes in the public interest. Safeguards are embedded in the Bill to ensure data is managed securely, including privacy protections, frameworks for risk management and transparency, and accreditation of data users and data service providers. The impact on the ease and ability to share data of the Data Availability and Transparency Act 2022 is still to be determined.

The bill is based around four key safeguards and include the use of the Five Safes Framework to manage the risks of reidentification. The four safeguards are as follows:

- Key safeguard: 1. Accreditation framework – to become accredited, an entity is required to have:
    - appropriate data management and governance policies and practices;
    - a qualified individual who has responsibility for data management;
    - ability to minimise the risk of unauthorised access, sharing or loss of data;
    - skills and capability to ensure the privacy and protection of data;
- Key safeguard: 2. Authorisations and penalties
    - The sharing can only occur if the sharer is satisfied that the sharing will be consistent with the "Five Safes" principles and the sharing is covered by a registered data sharing;
    - Penalty provisions can apply if there is unauthorised sharing or use of data.
- Key safeguard: 3. Privacy protections – key privacy protections and privacy-enhancing measures include:
    - data shared must not include personal information unless an exception applies;
    - a prohibition on the re-identification of de-identified data;
    - the storage of access of personal information should not occur outside of Australia;
- Key safeguard: 4. The National Data Commissioner
    - the Commissioner is responsible for overseeing and holding participants accountable to robust standards of privacy, security and transparency.

National Agricultural Statistics Review

The National Agricultural Statistics Review (NASR) talked to stakeholders of agricultural data throughout government and industry and made several recommendations to develop a best-practices agricultural data system *(ABS, 2015)*. Though the objective of the review was to reduce the survey burden on the agricultural sector, improving data sharing was determined to be a key component to reduce this burden by enabling the reuse of surveys for other purposes.

To this end, government and industry were widely consulted on the barriers to data sharing and key recommendations on data sharing included:

- Establishing a foundation dataset for agricultural statistics to provide a standard reference and serve a wide variety of users.
- Establishing an agricultural administrative data initiative to examine legislative, privacy and commercial barriers to the use of data collected by governments and industry.
- Encouraging a more coordinated approach from research funders in support of the agricultural statistical system.
- Establish a one-stop portal for agricultural statistics to maximise the value of existing data sources and provide discoverability and accessibility to the foundation agricultural dataset.

In 2018, ABS and ABARES held the second Agricultural Statistics Roundtable attended by state and federal government agencies and industry representative groups *(ABARES, 2018)*. There were several proposals for transforming data in agriculture, including:

- Common property identifiers in datasets: The ability to consistently link data collected on an individual farm to its physical location is expected to facilitate the integration of multiple data sources.

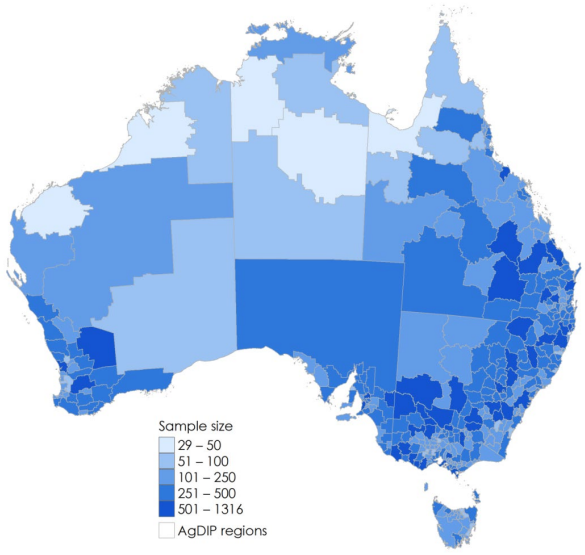
- Common metadata standards: The use of common metadata standards by agricultural data holders to improve the discoverability of data and facilitate the integration of multiple data sources.
- Harvesting farm management system data: Capturing relevant agricultural data directly from farm management systems for use in the production of statistics can reduce respondent burden in completing surveys.
- Integrated data platform: Consolidating available agricultural data captured by industry and government onto a single platform can reduce duplicative collection activities and improve the discoverability and accessibility of data.
- Harvesting industry levy data: The ability to use administrative data, such as agricultural levy data reported to the Department of Agriculture and Water Resources, can reduce respondent burden in completing surveys and provide more timely and accurate statistics for users.
- Surveys marketplace: A platform for industry and government stakeholders to advertise and search upcoming survey collections is expected to encourage greater collaboration among stakeholders.

Agricultural Data Integration Project

The Agricultural Data Integration Project (AgDIP) is a long-term collaboration between ABARES and the ABS to develop, integrate and analyse new farm-level agricultural data sets. This has led to the development of the Farm-level Longitudinal Agricultural Dataset (FLAD), which combines farm-level data from all ABS Agricultural surveys and censuses undertaken between 2000 and 2018.

The data is aggregated to AgDIP regions shown below, which have been chosen based on Statistical Area Level 2 (SA2) boundaries but modified so that no areas have fewer data points than a predetermined level. This project successfully integrated ABS data over different years; however, it did not integrate ABARES farm-level data or other data sources outside of the ABS *(ABARES, 2020)*.

Figure 1 – AgDIP data aggregation regions adapted from SA2 areas



Note: AgDIP regions are aggregations of ASGS 2016 SA1 regions that broadly respect SA2 boundaries, with some modifications to ensure reasonable farm sample sizes and to maintain consistency with AAGIS survey regions

2. Objectives

ExoFlare has been awarded a Traceability grant for the Cross-sector Operational Biosecurity Risk Assessment (COBRA) project to develop a real-time data driven approach to assessing biosecurity risks in the red meat and pork sectors. The objectives of the COBRA biosecurity traceability program over three years are as follows:

1. Determine key risks and opportunities for data sharing between government and commercial organisations;
2. Validate methods to capture data and provide notifications on biosecurity risks;
3. Recommendations on linking digital traceability and biosecurity risks;
4. Demonstrate risk communications and behavioural changes to improve biosecurity.

This larger project was planned into three phases. The first phase involved interviewing custodians of biosecurity data and other stakeholders to collect feedback and identify data sharing opportunities to determine the key risks and opportunities for data sharing between government and commercial organisations.

The first phase aims to understand how biosecurity data from across government and industry can be shared and analysed in new ways to improve our ability to manage existing risks and detect emerging risks sooner.

The objectives of this first phase, as discussed in this report, were the following:

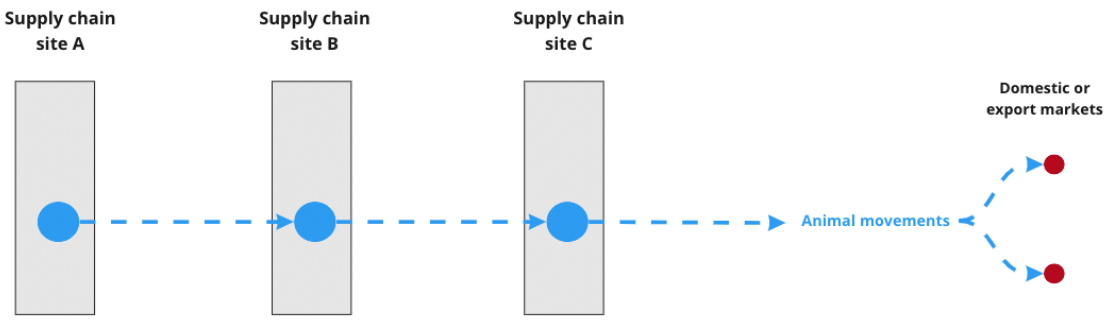
1. Validate ExoFlare's proposed biosecurity traceability vision and identify data resources of relevance;
2. Determine the blockers for sharing biosecurity data between organisations;
3. Find enablers that help organisations to share relevant biosecurity data;
4. Identify exemplar projects that showcase both the effectiveness of enablers and the benefits of data sharing.

3. Methodology and Results

ExoFlare conducted interviews with stakeholders involved in the Australian livestock biosecurity system to get feedback on the potential for a reimagined biosecurity traceability system that provides real-time information on biosecurity risks to industry and the data sharing required to enable such a system. In these interviews Exoflare presented participants with a broad overview of what a biosecurity traceability system could be. ExoFlare conducted 22 interviews that included the CVOs and key biosecurity officials of 5 states, key officials in 7 DAWE branches, and 4 other industry organisations. These contacts are considered custodians and stakeholders for the data relevant to managing biosecurity risk in the red meat and pork sector.

Figure 2 shows a simplistic supply chain with supply chain sites A, B, and C moving animals to either the domestic or export market. These sites could be for example a breeder, a backgrounder, and a feedlot.

Figure 2 – The traceability system with only animal movements recorded

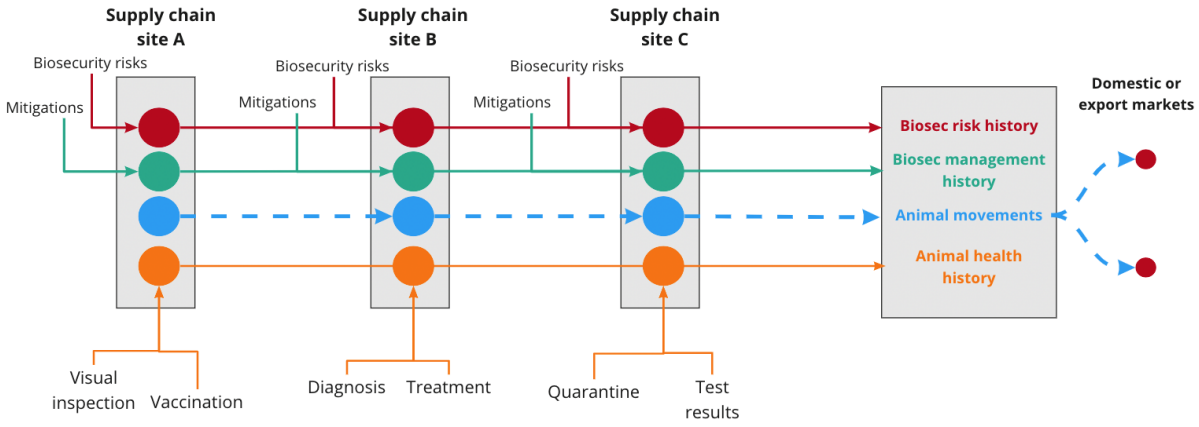


The current traceability system records information in the National Livestock Identification System (NLIS) on the movements of animals and specific disease and residue information, for the management of biosecurity by the government and to assure our export agreements.

ExoFlare proposed that in addition to the information on animal movements, they would also layer in data collected on the biosecurity risks, information on biosecurity management of those risks, and animal health history for each of these sites.

The aim of this system is to capture the data required to communicate real-time risk information to those best placed to respond, and in a form that they can use to drive decisions they are making in the moment. An important point here is that Exoflare intention is to capture this information from the supply chain, for the supply chain to understand and manage its own biosecurity. This would complement the current traceability system that assures export access and provides government vital information in Emergency Animal Disease (EAD) events.

Figure 3 – Traceability system with extended biosecurity risk and animal health information (ExoFlare analysis)



Mostly positive feedback was heard when this proposal was presented, with participants saying that while they have seen parts of this system, bringing all this data together and making it accessible in one place would be valuable. There was interest in the potential of data being used to drive and monitor behaviour change to improve biosecurity.

States saw real opportunities to use the data collected by this system and to send alerts for management during outbreaks. Exoflare found there was a new momentum to move to capture and share real-time data in this space. States are starting projects to define APIs (Application Programming Interfaces) for data that they have previously dealt with on paper. Federal government divisions are aware of the value of data and moving to improve their current systems with real-time data capture and analysis.

States were particularly interested in digitally collecting the information required for traceforward and traceback during EAD events. ExoFlare notes that sending information to the states even for defined purposes such as traceforward and traceback in an outbreak needs to respect the data rights of the industry. In particular, the Farm Data Code (NFF, 2020) stipulates that the farmer owns the data and any use or sharing of the data should be clearly communicated to them. Ideally the software would have the function to send data to state authorities but would only do this if the farmer proactively chooses such a function in the software and clear details of what is being shared with whom would be displayed.

3.1 Agreement on the importance of data sharing

Across all interviews and discussions, there were some common themes around the participants' experiences and perspectives on data sharing. Most participants agree that information sharing is a positive initiative and enables the Australian biosecurity system to function effectively. The Animal Health Committee is pointed to as an example of how open sharing of biosecurity information between the CVOs of the states allows early warnings of diseases to be shared and states to respond proactively to potential biosecurity risks.

> *"Data can generate and drive behaviour change. When you have data you have more idea about what you're actually doing, and you can quantify it, measure it, and monitor it. Then you can demonstrate the impact to other people."* *(Expert interview, 2022)*

There was general agreement that improved data sharing can lead to a better ability to manage existing and emerging biosecurity risks. This concords with several previous reports that have identified many significant benefits in being able to better utilise agricultural data *(KPMG, 2018) (MLA, 2016).*

3.2 Key data sharing risks

Participants were asked about the data they held that may be relevant to the system outlined in Figure 3. When asked if they would be able to share the data to enable such a system, participants brought up examples of where data sharing had previously gone wrong. These negative examples underpinned a risk-averse view of data sharing where it was likely for the data to be misused or misinterpreted.

Participants mentioned an instance when NLIS data had been shared for a research purpose but was then misused to find the optimal location for a new processing plant, giving commercial advantage from data originally collected for regulatory purposes. Additionally, examples were given of individuals who were identified publicly as having had notifiable diseases detected in their organisation's animals through data leaks. Even though there were very few instances of this, it was raised as being one of the worst outcomes of a data-sharing agreement. Agricultural communities are particularly sensitive to concerns of identification. For example, for feral animal sightings, landowners were concerned that identification could lead to illegal hunting of the feral animals on their land.

Through these examples and similar cases, the data provider could be exposed to key risks through the misinterpretation or misuse of shared data. There were 5 key risks that were raised when we discussed the consequences of the misuse or misunderstandings around data sharing.

1. *Protection of privacy*
   There are legal requirements that the data will not be disclosed to any other party unless it is for the primary purpose for which the data was collected.

2. *Commercial advantage*
   The agricultural industry is competitive, and the government needs to ensure that data is not misused.

3. *Reputation*
   Misunderstandings of data quality issues or misuse of data can reflect poorly on the data custodian.

4. *Trade impact*
   Biosecurity data has the potential to disrupt trade agreements and it is important for the government to carefully manage how any data is released to ensure the maintenance of trade relationships.

5. *Regulatory and contractual*
   Biosecurity data collected by DAWE falls under the Biosecurity Act 2015 and data collected or shared must comply with this act. For other areas, other regulation can apply such as the Export Control Act 2020 and the future Animal Rules Act 2021.

3.3 Data sharing barriers

There are processes in place to manage the risks identified in the previous section within all organisations Exoflare spoke to. However, most of the risks are based on anecdotal evidence and there is little evidence on the actual magnitude of the risks for different datasets. This has led to a risk aversion attitude to data sharing, and risk management processes that are biased in order to avoid these risks as much as possible.

Additionally, there is no global policy framework or operational guidelines for biosecurity data sharing that has been developed. This has led to data sharing processes being developed and managed independently for each organisation holding data.

Multiple barriers that impede data sharing have arisen from these risk management processes. In this section, the most common barriers to data sharing that ExoFlare has identified across governments below are described. Enablers that can help reduce and overcome barriers and enable improved data sharing are discussed in the next section.

3.3.1 Data is difficult to find or collate

While data is growing in importance, participants indicated a lack of knowledge both within and between federal and state governments on what biosecurity data is being collected and held. This limits data sharing as currently, groups wanting data need to know who manages the information they want before a data sharing request can be pursued. This was also a common theme of the government's previous agricultural data review, which raised the lack of discoverability of public and privately-held agricultural information and the lack of metadata to provide a clear, common understanding of the value of the data for a particular use case *(ABS, 2015)*.

This often arises as there are multiple programs in organisations that collect data related to that program's goals. These programs have different goals and therefore will collect data differently. In this case, the fragmentation of the data is aligned with the programs. Commonly, the data collected by each program is not clear, and there is little metadata available. This leads to an inability to find required data in other organisations or even in different branches of the same organisations. In addition to this, the fragmentation of the data across various projects and systems leads to data that cannot be collated, as the fields are incompatible or critical information is not measured in some of the projects.

Participants from the federal and state governments told anecdotally of planned improvements to biosecurity that were not implemented due to being unable to find pathways to share data. An example of this was a proposal to combine NLIS information with animal health information to enable improved health management; however, the data sharing required between states and federal departments was not achieved, and this proposal did not progress.

Another example was a state government that considered feeding back aggregated information around endemic disease incidence from state biosecurity laboratory testing data to industry, but this again did not progress due to the concerns around data sharing. Finally, states have investigated using data from private veterinary laboratories to collate endemic disease data that could be provided back to industry. However, the private laboratories view the risks of the government discovering potential notifiable diseases and contacting their clients as too great to provide the data.

Participants indicated that the federal government is unaware of data that state governments hold and vice versa. There is a similar lack of communication between states, highlighted by certain edge events where data is required by one state but held in another. One example is when a veterinarian visits a client in another state but sends a sample to their nominal laboratory in their home state. This means that the disease testing result for one state is held in the databases of another state.

A challenging issue is that unequal data collection leads to problems being found where data is collected. This not only disincentivises the industry to collect and share data, but also results in individual jurisdictions not sharing data that could be used to indicate that there are biosecurity problems in the area, compared to other areas that are not collecting data on the issue.

3.3.2 Concerns around data quality

Obtaining conclusions from data is complicated, and misunderstandings of how the data is collected, measured, or fits into the larger picture can lead to unsubstantiated claims or misleading results. Errors, missing data, and other data quality issues can lead to incorrect conclusions being made from this data and the potential for confusion and misinformation to come from government data. This has a high reputational risk to the government and can lead to unnecessary disruption to industry or trade.

Many groups spoke about quality issues in the data they collect and manage. This can involve missing data that has been failed to be entered, and data entered incorrectly. While some of these issues can be determined from inconsistencies in the data, the full extent of these issues is often unknown. This uncertainty over the quality of the data and the considerable domain knowledge required to make accurate decisions using messy data contributes to reluctance to share the data.

These can include data inaccuracies and errors taking on undue veracity due to the source of the information. This is particularly problematic for government departments where data collected from surveys of agricultural populations can contain erroneous data due to mistaken data entry or misunderstandings of the questions by the survey takers. This data, if released, can be mistaken to carry the stamp of approval of the department and could be used to make incorrect conclusions with a false sense of authority. This is a large concern of the government and means that they are careful to release raw data.

Examples were also given of data sharing where data was misinterpreted and had caused issues for the data owner. Often the data that the government collects is a sparse and biased sampling of the reality of the situation. For example, data on notifiable diseases is collected by the states, only if a vet or other member of public sees something that they are worried enough may be a notifiable disease. In this case, they are often sent a sample and test it for both notifiable diseases and exclusion testing for endemic diseases. This means that the samples collected are biased towards members of the public who are more concerned about biosecurity and who engage with veterinary experts.

Biased and sparse sampling of data can easily lead to underestimation of the actual spread and frequency of disease. More generally, there is an issue that data collected unequally across different areas can lead to the areas where data is collected, being reported to have higher levels of disease. Examples of this were raised by state governments, where higher levels of testing for disease has been used as evidence that these areas had more disease than others, which had been reported in academic publications without caveats or clearly explained context.

Issues around data quality were called out in the previous agricultural data review. The review noted issues around the relevance of data, with stakeholders indicating that 30% of data sources did not meet their needs, poor accuracy of data particularly related to low survey uptake, and the inconsistency of data sources in terms of measuring the same things over time and space *(ABS, 2015)*. Specific issues around the timeliness of data are discussed in the next section.

3.3.3 If shared, data is often not current or too coarse to be useful

In biosecurity data often there are multiple stakeholders in the data approval process which lead to long and complicated approvals. The current processes can require in-person meetings to sign off on the sharing of data, and discussion of potential consequences of the data shared. While this is an important step to mitigate risks of data sharing, particularly around trade impact and reputation loss, it is time consuming. For example, the collation and publication of notifiable disease information from all states is a semi-manual process that typically takes three months, from data collection to publication for the data from notifiable diseases and requires the sign-off of the Animal Health Committee to share the data publicly.

Other data sources from surveys of stakeholders or from data collected by local biosecurity management programs is not updated frequently. For example, management programs are still using national estimates of feral pig density from a study in 2008 and there is no clear picture for the total number of feral pigs in Australia today.

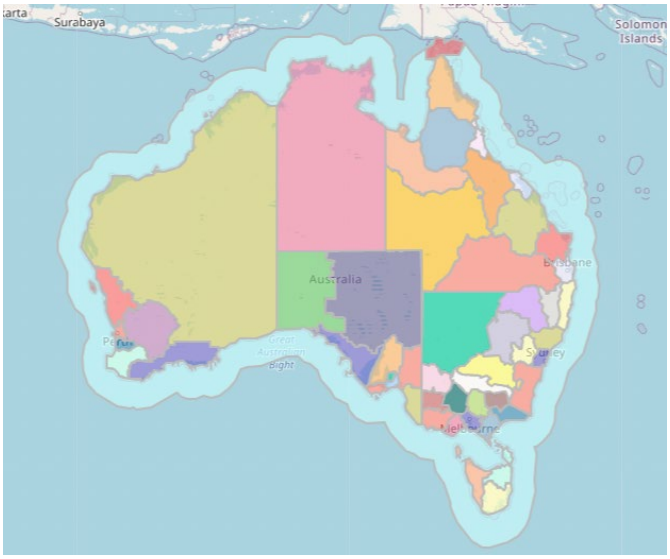
Exoflare heard when data is released it may not be a current enough picture of the situation on the ground to be useful. This leads to data that is not useful for managing biosecurity in real time. This can be contrasted to the communications that open when an outbreak occurs, when the state, territory, federal government, and other key stakeholders share information on the outbreak in real time. This is possible because of the resources allocated to the emergency response to not only collect and manage information but also to plan and respond directly.

Where there are biosecurity concerns that do not have an associated EAD response, the partnership between the livestock owners, veterinarians, and local, state, and national industry groups are responsible for the control and response to these biosecurity concerns. However, there is a gap between the collection of relevant information to inform an EAD response, and the information made available to those responsible for the preparedness and response to non-EAD biosecurity concerns, in a form that can be actioned.

Many agricultural datasets are aggregated to the 54 NRM (Natural Resource Management) regions in Australia. Participants pointed to the risk for re-identification of specific properties in sparse agricultural areas as the reason that this was done, in particular for Northern Territory and Western Australia where many agricultural properties are so large that they can be identified by species type and a postcode.

Not only must the privacy of the individual respondent be protected, but there are other blockers to sharing the data at a finer geographic level. Participants highlighted general contractual arrangements with the ABS to provide the locations of agricultural enterprises for various studies. The contract stipulated the shared data could not be used to derive insights from the data and this included aggregation that used the location of the agricultural premises. This effectively prevented any other spatial aggregation other than to the NRM level.

Figure 4 – NRM regions in Australia including the National Marine Region.



3.3.4 Complicated, legally intensive, and time-consuming data sharing process

There are no standard, one-size-fits-all processes to share biosecurity data held by the federal government, state governments, or other data-holding organisations. Participants called out that policies are still being developed for data sharing and that it is a current grey area. Typically access to data requires negotiation with the data custodian, with the process generally involving the following steps:

1. identifying the purpose of the request for data;
2. determining if the providing organisation has the data requested;
3. deciding if the data can legally be used for the purpose requested;
4. identifying specific considerations and blockers for sharing the data;
5. finally determining paths forward, identifying how the blockers can be overcome.

All these parts of the process are data-specific and require the involvement of legal and subject matter experts to determine the specific risks. This unfortunately leads to the process often taking many months for each data sharing request. Participants called out that policies are still being developed for data sharing and that it is a current grey area.

> *"Access to data is difficult even for us in the department. The new Export Control Act 2020 and Animal Rules Act 2021 make data access even tighter and more restrictive." (Expert interview, 2021)*

The main policy that must be fulfilled by the department to share biosecurity information is the Biosecurity Act. Additionally, there are responsibilities around identifiable information in the Privacy Act 1988. All participants were concerned with preventing leaks of identifiable information or re-identification of individuals or businesses in their datasets. In addition, new regulations such as the Export Control Act 2020 and Animal Rules Act 2021 must be identified and considered in data sharing negotiations.

These restrictions have led to livestock enterprises having difficulties accessing information directly relevant to their properties' biosecurity due to access restrictions. External organisations are sometimes tasked with gathering data for regulatory purposes and, in parallel, collecting commercial information. This leads to complex questions of data ownership and access rights and often causes significant technical and legal issues around who can access what information in the same database. This has caused government branches to have difficulty accessing data that was collected by these external organisations in the same process used for the collection of regulatory information passed to the government.

3.3.5 Technically challenging to share data

The barriers discussed previously lead to data sharing not being a regular occurrence. It is not surprising then that the data systems reflect this and do not support easy data sharing. The challenges in sharing data also mean that data required by an organisation can be collected and analysed independently from the system, and often duplicates efforts in other divisions and organisations. These factors lead to the systems being fragmented and incompatible.

A common issue reported by participants was that older systems make data sharing a manual and time-consuming process. These older systems are difficult to use, only allowing manual exports of data for specific time periods and require a sophisticated understanding of the specific system. There is a lack of digital systems that provide APIs for permissioned access that would allow continuous updates to previous analyses utilising a consistent data source. Exoflare also heard that there is a lack of user-friendly systems to collect data in a way that allows real-time updates of databases.

ExoFlare found that while there were projects starting to modernise how data is collected and handled, these projects are moving slowly and there was not a strong sense of significant movement in this area.

These issues lead to insights derived from biosecurity data only capturing a single point in time and area of interest. If these insights need to be updated, the process of data negotiation, manual data exports, data cleaning, collation, and analysis needs to be redone in addition to the approval processes for these insights to be released outside the originating organisation. This means there is significant time and effort required each time data insights are refreshed, leading to a long lag time with data collection, and very few programs going through the effort to update these insights.

Participants pointed to stakeholders developing their own data collection tools and standards independently leading to further fragmentation and siloing of data. An example of this is feral animal data where different management projects collect data mostly around the number of animals culled in management programs. Currently each jurisdiction handles this differently with some having an integrated system where data from multiple programs is available and others where systems are splintered and are not integrated. For example, NSW feral pig data is available in a central system whereas the QLD feral pig programs are managed by the local councils who collect and manage data independently, with different data standards in each council.

In addition to managing data independently, states are also developing their own data collection tools and standards independently. For example, the National Parks and Wildlife Services in multiple states are developing apps to collect data on their management programs independently that will capture data for their own systems.

These themes have been surfaced by the government in its review of agricultural data and statistics *(NASR, 2015)*. In particular, the review reported that there are different systems and techniques used to collect, analyse, and disseminate data throughout the agricultural system and that these are not shared. This has resulted in siloed systems and duplication of effort to collect and analyse the same data. This theme appears to continue, with many participants citing plans for the development of separate digital data collection platforms.

3.4 Enablers for data sharing

While data sharing is seen as key to the functioning of the biosecurity system, data sharing beyond the currently identified channels is often not a priority in many departments. This parallels the development of data.gov.au, the government's own open data platform where open data was not seen as a priority in government until the benefits of open data were highlighted.

> *"When we could show a department the specific benefit to them – which often in the first instance would be some form of financial benefit or cost saving – they would come for the efficiency but stay for the innovation." (Salsa Digital, 2022)*

These risks and barriers are not new, ExoFlare are certainly not the first to investigate this area. There has been extensive research in this area and there are many processes and technologies that can help with some of these barriers without increasing the exposure to the five risks.

Exoflare have not tried to propose new solutions to these barriers but have identified several exemplar projects that have successfully tackled some of them, and tools that have been developed to manage them.

3.4.1 Simplify data sharing negotiation process

The current process for obtaining access to data is often not clear for the data requestor or the data custodian. There is potential to simplify the data sharing negotiation process in certain use cases

where the risks for sharing the data have been identified and a management plan is established. After this request, data access can be processed focussing on the purpose for which the data is requested and determining if this aligns that for the data collection and being able to review the risks of this risks using pre-determined metrics. This takes the position that data will be shared, and therefore the legal work to identify the risks around each dataset is performed upfront with that in mind.

Queensland Data Transfer Agreement

An example of this is, the Queensland Government has recently introduced a standard data sharing agreement template used to start data sharing requests with the Queensland Government for a variety of datasets and situations. This has reduced the time to fulfil data sharing requests from many months to less than a month and could be a model for other states and organisations in the future.

3.4.2 Move to online processes for permissioned data sharing sign-off

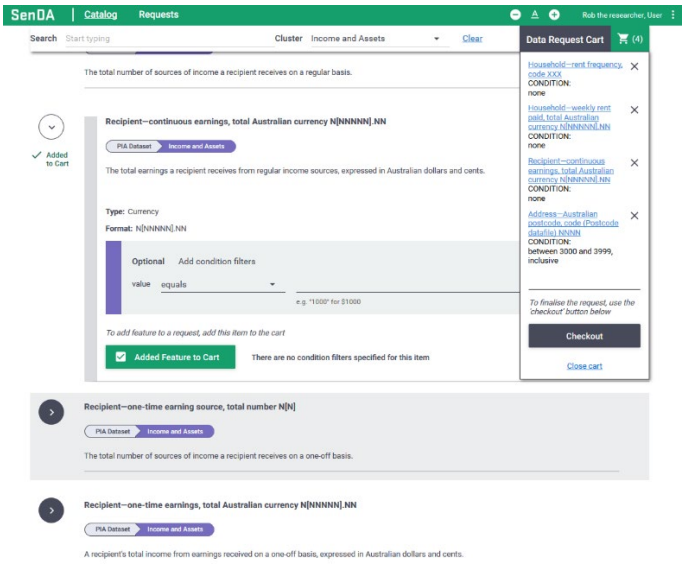
Moving to an online platform to enable online, permissioned data sharing sign-off can reduce delays in new data sharing releases. This contrasts to the current process where data releases are either ad-hoc or require meetings of all stakeholders to agree for the data to be released.

SenDA Platform

The Sensitive Data Access (SendDA) platform was developed by CSIRO's Data61 for Commonwealth agencies to digitise and streamline the process of permissioned data access, leave audit trails, and review past approvals. SenDA allows requesters to create and update fine-grained requests for data, curators to approve or reject them, and both to engage in a dialogue, allowing them to negotiate data access that satisfies both parties. The request process is tracked and able to be audited, providing certainty and accountability to both data curators and those requesting data.

SenDA is designed to replace parts of the existing, largely offline or email-based workflow for obtaining sensitive granular data for research or analysis, with the ultimate goal of reducing the time and effort required to obtain access to such data.

Figure 5 – The Sensitive Data Access (SendDA) platform



3.4.3 Use tools to manage the risk of reidentification

Shared data is often required to be de-identified or otherwise transformed in a way that reduces the risk of privacy breaches, while still maintaining the value of the data for its intended purpose. There are a multitude of methods for maintaining privacy while enabling the data to be used for analysis, from simple to exceedingly complicated.

The details of how to apply these methods and their risks to reidentification are provided in the De-identification and the Privacy Act report by the Office of the Australian Information Commissioner *(OAIC, 2018)* and the ABS Data confidentiality guide *(ABS, 2021)*. These methods for de-identification include:

Deidentification

- This removes sensitive data fields that can directly be used to identify an entity, such as the name of a person or the name and location of an agricultural enterprise.
- In some cases, sensitive data fields can include those that would provide important information to the analysis; for example, the location of a data point is sensitive but also provides important information for geographic differences in the data being measured.
- There are significant risks to re-identification if the data point is unique in the non-sensitive fields.

Data perturbation

- This perturbs the fields of each data point in such a way that the privacy of the individual response is maintained while the data is still statistically useful. For example, the location is randomly changed enough for the data point to not be able to be tied to a specific agricultural enterprise.
- There are risks to re-identification if the perturbation is not done carefully, or there are data points that are still unique even after perturbation.

Aggregation

- Aggregation combines multiple data points into a single, representative data point. An example is combining data within certain geographic regions to provide a statistical representation of that area.
- The risks to re-identification are related to the number of data points that are combined.

Modelling

- In some cases, models can be developed that are driven by the statistics of real data and are then used to generate synthetic datasets that are representative of the real data collected.
- These models can be quite resistant to privacy breaches; however, the data that they produce is only as valid as the model used to generate it. There can be assumptions made in the modelling that lose important aspects of the input data; for example, outliers may be ignored in model fitting but provide key insights to rare events.

Privacy preserving analytics

- New techniques have emerged in recent years that allow data to be shared in an encrypted fashion. This is the most complicated of the techniques and requires new algorithms to

> analyse and extract insights from the encrypted data. However, this has an enormous potential for extracting insights from data with privacy guarantees *(Microsoft, 2021)*

For each of the de-identification techniques, there is a risk that either the data can be re-identified or that some information about an entity can be inferred using some known properties of the entity. There are tools to help manage the risk of re-identification that quantify the risk for a particular dataset.

Re- identification Risk Ready Reckoner (R4)

Data61's Re-identification Risk Ready Reckoner (R4) allows a de-identification or aggregation scheme to be chosen based on a quantification of the risk level. For deidentification and perturbation methods, R4 provides a measure of the re-identification risk for an individual event or transaction based on factors such as uniqueness, uniformity and/or linkability. For aggregation methods, R4 can calculate the risk of deducing a non-reported value in the aggregated data report.

Finally, there are detailed guides on making decisions on the release of de-identified data, such as the De-Identification Decision-Making Framework from CSIRO and the Office of the Australian information Commissioner *(OAIC, 2017)*.

3.4.4 Standardise data collected for biosecurity management projects

Fragmented and siloed data is often a result of biosecurity projects with different goals, collecting different data that maps to those goals. Standardising data collected for biosecurity management projects can help to alleviate this, which aligns with the recommendation of the National Agricultural Statistics Review (NASR) to pursue a coordinated approach from research funders in support of the agricultural statistical system *(ABS, 2015)*.

National Feral Pig Action Plan (NFPAP)

For example, the NFPAP has recommendations for data collection standards to be required in new grants for the control of feral pigs to ensure that data is collected in a way that can be collated across projects and be used to quantify the overall goals of the program. The plan recognises the importance of data in driving decisions and sets out ways to organise feral pig management to collate improve data and use this to both quantify the goals of the national project and make better decisions in managing feral pig populations. *(NFPAP, 2021)*

Health 4 Wealth Programme

This programme developed a standardized approach to data collection on disease-related carcase and offal condemnations and a nationally agreed, consistent feedback system for livestock producers. The project has demonstrated that individual carcase disease and defect data can be shared from beef abattoirs to producers through online services (*MLA,2021*).

A particular focus has been on standardising the disease and defect data between abattoirs leading to the National Standard for the Development, Collection and Reporting of Animal Health Data *(RMSCC, 2016)*. This has led to significant cost savings in moving from paper-based to digital reporting systems of disease and defect data (*MLA,2021*).

3.4.5 Leverage existing data-sharing frameworks

Data sharing frameworks have been used successfully to catalogue datasets over different organisations in a federated way, not only providing the datasets that have been collected but also capturing key metadata about the data held to improve the ability to find required data. For example, CKAN is an open-source software project used for indexing open data directories and underpins the data.gov.au portal and multiple state data portals.

The experience of the data.gov.au portal was around creating an improved culture of data sharing by highlighting efficiencies for the agencies involved, which then transformed how the system worked through the innovations that evolved once data was available *(Salsa Digital, 2022)*. A similar story can be told about the National Map geospatial hub that collates data from all states around Australia, connects to their different APIs, and provides a consistent, harmonised view of geospatial data.

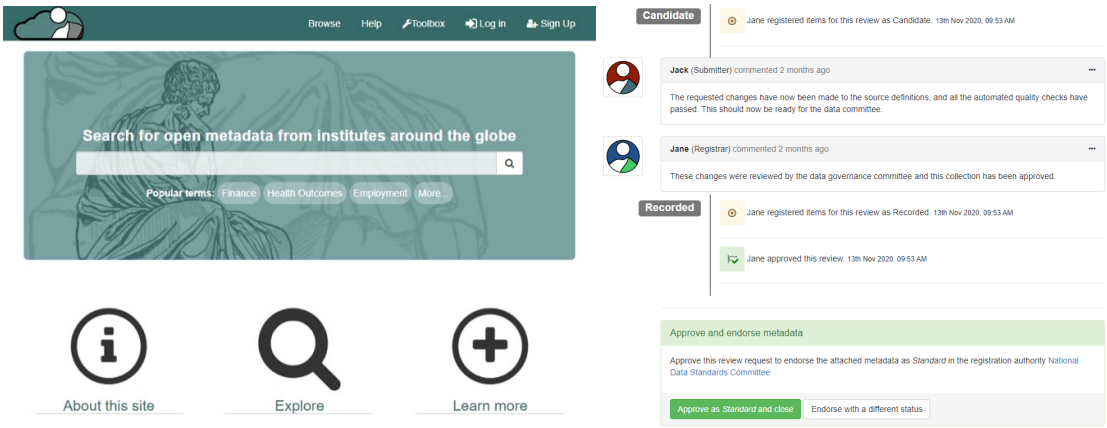
These themes have been surfaced by the government in its review of agricultural data and statistics *(NASR, 2015)*. The review recommended the promotion of a culture of open data as well as providing a one-stop portal for agricultural data as important next steps toward a best practice agricultural data system for Australia. In addition, the second Agricultural Statistics Roundtable called out the establishment of Common metadata standards to improve the discoverability of data *(ABARES, 2018)*.

Aristotle metadata registry

After noting that many statistical and data-oriented agencies around the world had built bespoke systems based on the ISO/IEC 11179 metadata registry standard. Each of these organisations had gone about solving and re-solving this problem, but there was a reluctance to share systems due to the perceived risks of government agencies providing commercial software.

The Aristotle metadata registry provides a central registry that brings together knowledge of data assets in a system ready to integrate with your data environment. It additionally provides tools to integrate with business processes and manage metadata access permissions.

Figure 6 – The Aristotle metadata registry



3.4.6 Develop interoperability through APIs and long-term permissioned data access

A common issue in sharing data was older systems that make it difficult to collect data in a timely fashion and make data sharing a manual and time-consuming process. These older systems only allow manual dumps of data for specific time periods, are difficult to use, and require a sophisticated understanding of the specific system. At the same time, ExoFlare has found that the government and agricultural industry have multiple projects that aim to modernise data analysis, collection, and sharing. This reflects the growing awareness of the importance of data-driven alerting and monitoring systems to enable improved detection and fast response to biosecurity threats. The data modernisation efforts are focusing on moving to digital data capture from paper-based collection, data standardisation, and increasing real-time data capture and analysis.

Data standardisation is being improved through digital apps that guide users through data entry and allow easy capture of extended information such as photos and videos, and improved training for how to enter data. An example is the Rangers App used for biosecurity data collection by the North Australian Quarantine Survey (NAQS).

Improvements in data analysis are being pursued in multiple areas including moving to modern cloud-based data systems such as Power BI. For example, the government and industry formed the Meat Modernisation Working Group (MMWG) to modernise the analysis and communication of meat industry data. Projects in this working group include the use of Power BI to provide dashboards with key information along with a project that looks at moving to real-time data entry. Also, DAWE's Biosecurity Strategy & Analytics Division is building data pipelines to clean and join data held across DAWE and in other departments, providing clean and usable data to answer specific strategy and policy questions. Teams from the Biosecurity Strategy & Analytics Division, Meat Export Group, and the Live Export Division are building systems to clean and integrate multiple data sources and provide dashboards to give up-to-date insights that the department can use on an ongoing basis to answer specific strategy and policy questions.

For the red-meat industry, Integrity Systems Company (ISC) has developed a new eNVD graphQL API which allows finely permissioned data access and entry to the eNVD database allowing the creation, modification and retrieval of data inefficiently. This enables other solutions to be built for both government and other stakeholders to have ongoing access to the data that they are approved to access, to enable ongoing updates to insights derived from this data.

ExoFlare found that there is an opportunity to establish standardised protocols for digital biosecurity traceability data to state and territory government biosecurity offices. Such information includes digital records of visitors to the site that can be used for traceforward and traceback during EAD events. Establishing standardised protocols for transmission of such data to all state and territory biosecurity offices will enable the interoperability of current and future digital products across Australia with the risk that if this is not done each state and territory will develop competing and incompatible protocols.

Australian AgriFood Data Exchange

Multiple stakeholders in the agricultural sector including government, science and industry bodies are collaborating to establish the Australian AgriFood Data Exchange. With a vision to establish an open data platform controlled by users, this data exchange plans to act as a trusted and secure platform for the exchange of agricultural data between organisations within the agriculture supply chain. Importantly the promotion of this data sharing culture would be backed by an established data governance framework, including protocols and policies for data access, privacy, definition and standards.

This project aims to provide an integrated data exchange that can enable the sharing of data in industry. Recent demonstrations from multiple projects have shown that existing data sharing infrastructures can be adapted to the needs of agricultural data sharing and allow fine-grained permissions and access given on an as-needs basis to both government departments, assurance programs, and other supply chain partners through a standard API.

4. Conclusion

ExoFlare have found that there is general agreement on the opportunity provided by easier data sharing, to improve biosecurity afforded by sharing data. With a vision of a biosecurity traceability system as a talking point, the barriers to sharing data that could make that goal a reality were discovered.

The main barriers relate to navigating a complicated and time-consuming data sharing process which can take months for each data request, and cost considerable resources for both the data requestor and the data provider. ExoFlare identified that opportunities to improve biosecurity have been missed, due to the inability to share data and there is an ongoing difficulty finding out what data is collected and held by whom in the Australian biosecurity system.

ExoFlare found many stakeholders still related similar barriers to those that have been identified in previous studies of the agricultural data system and that there has been little progress against the recommendations made in previous reports *(ABS, 2015)*. The barriers remaining include the difficulty finding relevant data for biosecurity projects, concerns around data quality, and the data that was shared was often not current or too coarse to be useful. In addition, older systems are still in use and participants reported exporting data with these systems is difficult and time-consuming.

However, there are new projects in both government and industry that aim to improve data sharing and integration. Within the federal government the Meat Modernisation Working Group (MMWG) is transforming data analysis pipelines to use cloud-based solutions. These cloud-based platforms enable multiple data visualisation and analysis tasks to be done quickly and by domain experts without the need for coding expertise. The MMWG plan to use this capacity to realise more value from the data they have and to use data more broadly in their decision making.

Divisions from DAWE's Biosecurity Strategy & Analytics Division, Meat Export Group, and the Live Export Division are building systems to clean and integrate multiple data sources and provide dashboards to give up-to-date insights that the department can use on an ongoing basis to answer specific strategy and policy questions.

5. Future research and recommendations

To realise the proposed biosecurity traceability system, the following should be pursued:

1. Federal, state, and territory governments should pursue improvements in data sharing by following the recommendations of the National Agricultural Statistics Review *(ABS, 2015)* and the suggestions in the second Agricultural Statistics Roundtable *(ABARES, 2018)*.
2. Industry bodies should continue with projects to enable permissioned exchange of agricultural data such as the Australian AgriFood Data Exchange project to enable management of biosecurity by the supply chain.
3. Use existing solutions for data release risk management and permissioned data access to improve data sharing within federal government departments and between federal and state governments.
4. Pursue further research into connecting risk information through the supply chain to enable a real-time, data-driven approach to assess networked biosecurity risk for the red-meat industry.
5. Establish standardised protocols for digital biosecurity traceability data to state and territory government biosecurity offices. Such information includes digital records of visitors to the site that can be used for traceforward and traceback during EAD events.
6. Establish an open-data platform to collate real-time aggregated biosecurity risk information derived from government and private data.

6. References

(ABARES, 2018)

The outcomes of the second Agricultural Statistics Roundtable, Australian Bureau of Statistics (ABS) and ABARES, 2018

https://www.awe.gov.au/abares/data/improving-agricultural-statistics/stakeholder-engagement

(ABARES, 2020)

The Agricultural Data Integration Project, Neal Hughes, Mihir Gupta, Wei Ying Soh, Chris Boult, Kenton Lawson, Michael Lu, Tim Westwood, ABARES

https://www.awe.gov.au/abares/research-topics/climate/agricultural-data-integration-project

(ABS, 2015)

National Agricultural Statistics Review (NASR), Document number 7105.0.55.004, Australian Bureau of Statistics (ABS), 2015

https://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/7105.0.55.004Main+Features12015

(ABS, 2021)

ABS Data confidentiality guide, Australian Bureau of Statistics (ABS), 2021

https://www.abs.gov.au/about/data-services/data-confidentiality-guide

(ARDC, 2016)

FAIR Guiding Principles for scientific data management and stewardship, Australian Research Data Commons, 2016

https://ardc.edu.au/resources/aboutdata/fair-data/

(AGPC, 2017)

Productivity Commission Inquiry Report Data Availability and Use Overview & Recommendations, Australian Government Productivity Commission, 2017

https://www.pc.gov.au/inquiries/completed/data-access/report/data-access-overview.pdf

(CSIRO, 2020)

Australia's Biosecurity Future: Unlocking the next decade of resilience (2020–2030), CSIRO, 2020

https://www.csiro.au/en/work-with-us/industries/health/health/biosecurity-futures

(DPMC, 2015)

Australian Government Public Data Policy Statement, Department of the Prime Minister and Cabinet, 2015

https://www.pmc.gov.au/resource-centre/public-data/australian-government-public-data-policy-statement

(KPMG, 2018)

Talking 2030: Growing agriculture into a $100 billion industry, KPGM, 2018

https://home.kpmg/au/en/home/insights/2018/03/talking-2030-growing-australian-agriculture-industry.html

(Microsoft, 2021)

Privacy Preserving Machine Learning: Maintaining confidentiality and preserving trust, Microsoft Research Blog, 2021

https://www.microsoft.com/en-us/research/blog/privacy-preserving-machine-learning-maintaining-confidentiality-and-preserving-trust

(MLA, 2016)

Beef Genetics RD&E Priorities 2016 – 2021: An industry consultation paper prepared by the Genetics RD&E Steering Group, Meat and Livestock Australia, 2016

https://www.mla.com.au/research-and-development/Genetics-and-breeding/NLGC-National-Livestock-Genetics-Consortium/

(MLA, 2021)

2021 State of the industry report: The Australian red meat and livestock industry. Meat and Livestock Australia, 2021.

https://www.mla.com.au/globalassets/mla-corporate/prices--markets/documents/trends--analysis/soti-report/2789-mla-state-of-industry-report-2021_d11_single.pdf

(NFF, 2020)

Australian Farm Data Code, Edition 1. National Farmers Federation, 2020.

https://nff.org.au/programs/data-and-connectivity

(NFPAP, 2021)

National Feral Pig Action Plan: 2021 – 2031, Australian Pork Limited, 2021

https://feralpigs.com.au/the-plan

(OAIC, 2017)

De-Identification Decision-Making Framework, CSIRO and the Office of the Australian information Commissioner (OAIC), 2017

https://data61.csiro.au/en/Our-Research/Our-Work/Safety-and-Security/Privacy-Preservation/De-identification-Decision-Making-Framework

(OAIC, 2018)

De-identification and the Privacy Act, Office of the Australian Information Commissioner, 2018

https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act

(ONDC, 2022)

The Data Availability and Transparency Act, Australian Government Office of the National Data Commissioner, 2022

https://www.datacommissioner.gov.au/data-legislation/data-availability-and-transparency-act

(Salsa Digital, 2022)

Open data: come for the efficiencies, stay for the innovation, Emil Jeyaratnam, Salsa Digital, 2022

https://salsadigital.com.au/insights/open-data-come-efficiencies-stay-innovation

(Wilkinson, 2016)

The FAIR Guiding Principles for scientific data management and stewardship. Wilkinson, M., et al., Sci Data 3, 2016.
https://www.nature.com/articles/sdata201618