



Australian Government
Department of Defence

DEFENCE DATA STRATEGY

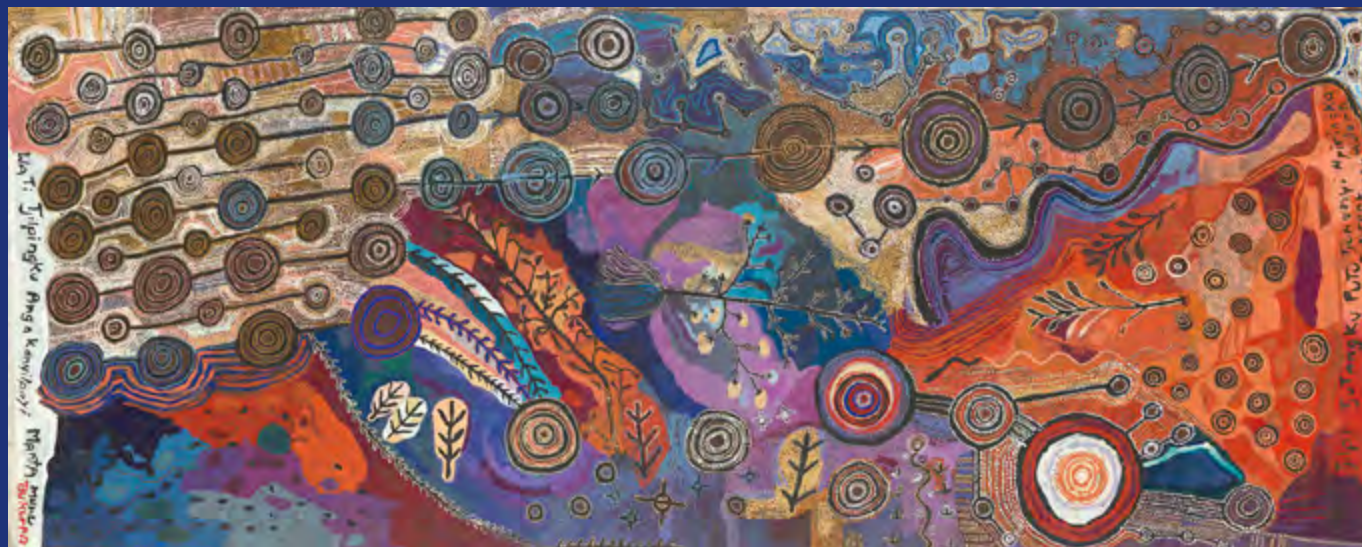
2021–2023



Acknowledgements

Defence acknowledges the Traditional Custodians of the lands, seas, and air in which we live, work, and train. We pay our respects to their Elders past, present, and emerging. We also pay our respects to the Aboriginal and Torres Strait Islander men and women who have contributed to the defence of Australia in times of peace and war.

The creative design of the *Defence Data Strategy 2021-2023* has been inspired by 'Kulatangu angakanyini manta munu Tjukurpa' (Country and Culture will be protected by spears).



The artists below include the names of deceased Aboriginal and Torres Strait Islander peoples.

The artwork was created by 19 senior male artists of the Anangu Pitjantjatjara Yankunytjatjara (APY) Lands, Nyapari, South Australia in 2017. The artists are: Alec Baker; Eric Kumanara Mungi Barney; Pepai Jangala Carroll; Taylor Cooper; Witjiti George; Willy Kaika; Kunmanara (Brenton) Ken; Kunmanara (Ray) Ken; Dickie Marshall; Kunmanara (Willy Muntjanti) Martin; Peter Mungkuri; Kunmanara (Jimmy) Pompey; Keith Stevens; Bernard Tjalkuri; Thomas Ilytjari Tjilya; Ginger Wikilyiri; Mick Wikilyiri; Kunmanara (Mumu Mike) Williams; and Frank Young. The Department of Defence thanks the artists and the APY Art Centre Collective Gallery for their work and the permission to use it as the inspiration for the *Defence Data Strategy 2021-2023* design.

This artwork must not be reproduced without permission. Further information on this artwork can be found at: [Kulatangu angakanyini manta munu Tjukurpa \[Country and Culture will be protected by spears\] | Australian War Memorial \(awm.gov.au\)](https://www.awm.gov.au/kulatangu-angakanyini-manta-munu-tjukurpa).

Defence would also like to acknowledge everyone across the enterprise who contributed to the development of the *Defence Data Strategy 2021-2023* for sharing their experiences, knowledge, and time generously.

© Commonwealth of Australia 2021

ISBN: 978-1-925890-46-4

This work is copyright. Apart from use as permitted under the Copyright Act 1968, no part may be reproduced by any process without prior written permission from the Department of Defence.

Foreword

The Government's key priority is to keep our nation safe and protect our way of life for future generations.

With this in mind, I welcome the release of the *Defence Data Strategy 2021-2023*.

Increasingly, the effective use and management of data will be critical to the successful conduct of Defence operations, in times of conflict and in peace.

This Strategy will guide data management and improve data literacy across the Defence organisation. This is critical to underpinning Defence's mission-focus.

As we know from the *2020 Defence Strategic Update*, and the *Defence Transformation Strategy*, lifting Defence's data maturity and leveraging it across the organisation will ensure we achieve a strategic advantage over our adversaries.

We are straddling vast change in the Indo-Pacific region. The next decade will bring greater geostrategic competition between nation states along with increased military modernisation. Grey zone tactics are now being used to coerce states below the threshold of conventional war. The risks to Australia are concerning.

We live in a data-rich world in a digital age. Cyber espionage and warfare are a reality that we cannot ignore. Whether we like it or not, we are joined in an online contest to preserve our personal security and our digital sovereignty as a country.

This Strategy will enable Defence's capacity to use data more effectively as our strategic circumstances change.

As noted in the *Defence Transformation Strategy*, our Defence culture must recognise the criticality of data to everything that we do, and adopt a disciplined and deliberate approach to how information is collected, stored, analysed and applied in decision-making processes.

This is what the *Defence Data Strategy 2021-2023* seeks to achieve.

I commend it to you.

The Hon. Andrew Hastie MP
Assistant Minister for Defence



A joint message from the Associate Secretary and Vice Chief of Defence Force

The world is experiencing rapid changes in digitisation and exponential growth in the creation of data. In response, organisations across the government, non-government and industry sectors are increasing their investment in data management to exploit new opportunities, provide better services and increase the value they deliver to key stakeholders.

Defence holds many data assets across the enterprise, ranging from Defence mission and operational data, through to policy and corporate enabling data. Improving data management will enhance our ability to be successful in an era of geostrategic competition. It will enable warfighters to capitalise on strategic and tactical opportunities that are currently unavailable in a fragmented data environment. It will help us better understand our capacity and build a more resilient Defence enterprise.

We have a responsibility to harness the potential of our data and leverage it across the organisation to achieve strategic advantage over our competitors. In doing so, we must increase the quality of our decision-making capability. This will directly impact on our ability to *defend Australia and its national interests, in order to advance Australia's security and prosperity*. Our ability to remain competitive depends on us becoming leaders in operationalising our data at speed and scale.

To become a more data-informed organisation and improve our ability to influence through evidence-based advice, we are pleased to present the *Defence Data Strategy 2021-2023* (the *Defence Data Strategy*). The *Defence Data Strategy* outlines Defence's vision for data, the pillars that will support us on our journey – *Govern, Trust, Discover, Use, and Share*, and the foundational initiatives required to achieve our vision.

We will value our data and remove barriers for Defence personnel to access and use it well. We will develop a Defence culture that puts data at the centre of our decision-making.

This *Defence Data Strategy* is a call to all Defence personnel – no matter what level or rank. It is our collective responsibility to lift our organisation's data maturity to ensure we can continue to deliver on the Defence Mission.



Katherine Jones PSM

Associate Secretary, Department of Defence



Vice Admiral David Johnston AO RAN

Vice Chief of the Defence Force



TABLE OF CONTENTS

Purpose	9
Australia's changing strategic environment: through a data lens	12
A vision for Defence data in 2023	13
Our Partners	16
What is data?	18
Our Data Challenge	20
Our Data Maturity	21
Pillars	25
1. Govern	26
2. Trust	31
3. Discover	34
4. Use	38
5. Share	41
Priority data areas	45
Measuring Success	50
Implementation Roadmap	52

Corporal Meg Reeves uses a Ghost Robotics quadruped for a reconnaissance task, 2021.
Photo Credit: Sergeant Jake Sims.



Purpose

To achieve the Defence Mission, we must optimise the strategic, operational and tactical use of our data assets. The foundation of this is improved data management practices. This will enable Defence to access the right information at the right time to support decision-makers.

Defence Mission: To defend Australia and its national interests in order to advance Australia's security and prosperity.

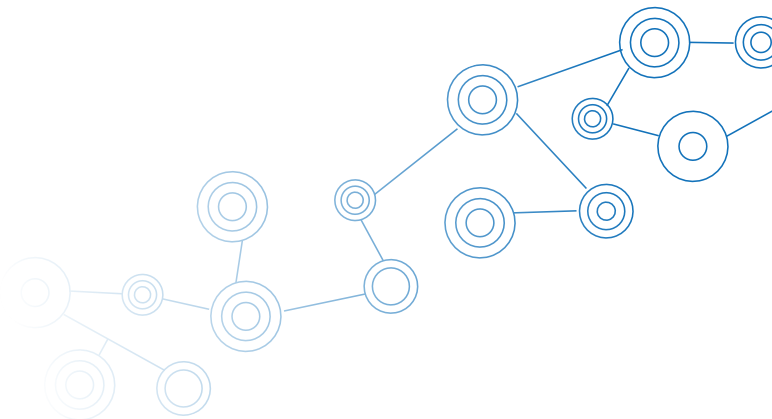
Recognising data as an asset means taking responsibility for it and understanding that it has inherent quantifiable value to our organisation and to others. Harnessing our data will allow us to take decisions and actions that are backed by information and insights gained through good data management. It will give us a strategic advantage over our competitors, make us a more effective fighting force and further support the **strategic centre** through improved decision-making.

The **strategic centre** includes the Defence leadership and governance and accountability arrangements that support our capacity to make informed decisions and to ensure these decisions deliver on agreed policy and strategy.

The **Defence enterprise** encompasses all of the Groups and Services within the Department of Defence, and their associated people, functions, and outputs. The shared outcome that we generate is our achievement of the Defence Mission through the Defence strategic objectives (shape, deter, respond), and the strategic effects outlined in the classified *Defence Planning Guidance*.

Through the development of the *Lead the Way: Defence Transformation Strategy*, senior leaders emphasised that Defence must recognise the criticality of data. The *Defence Data Strategy* sets out the vision, pillars, practical initiatives and priority data areas to lift our data maturity and work towards becoming a more data-informed organisation.

We will embed data literacy as a cultural norm and put useful and trusted information at the centre of everything we do. The *Defence Data Strategy* commits Defence to implementing foundational enterprise-wide data initiatives. It will deliver investment in leadership, data management and in our people.



The *Defence Data Strategy* covers all digitised data in Defence, both structured and unstructured. This includes, but is not limited to:

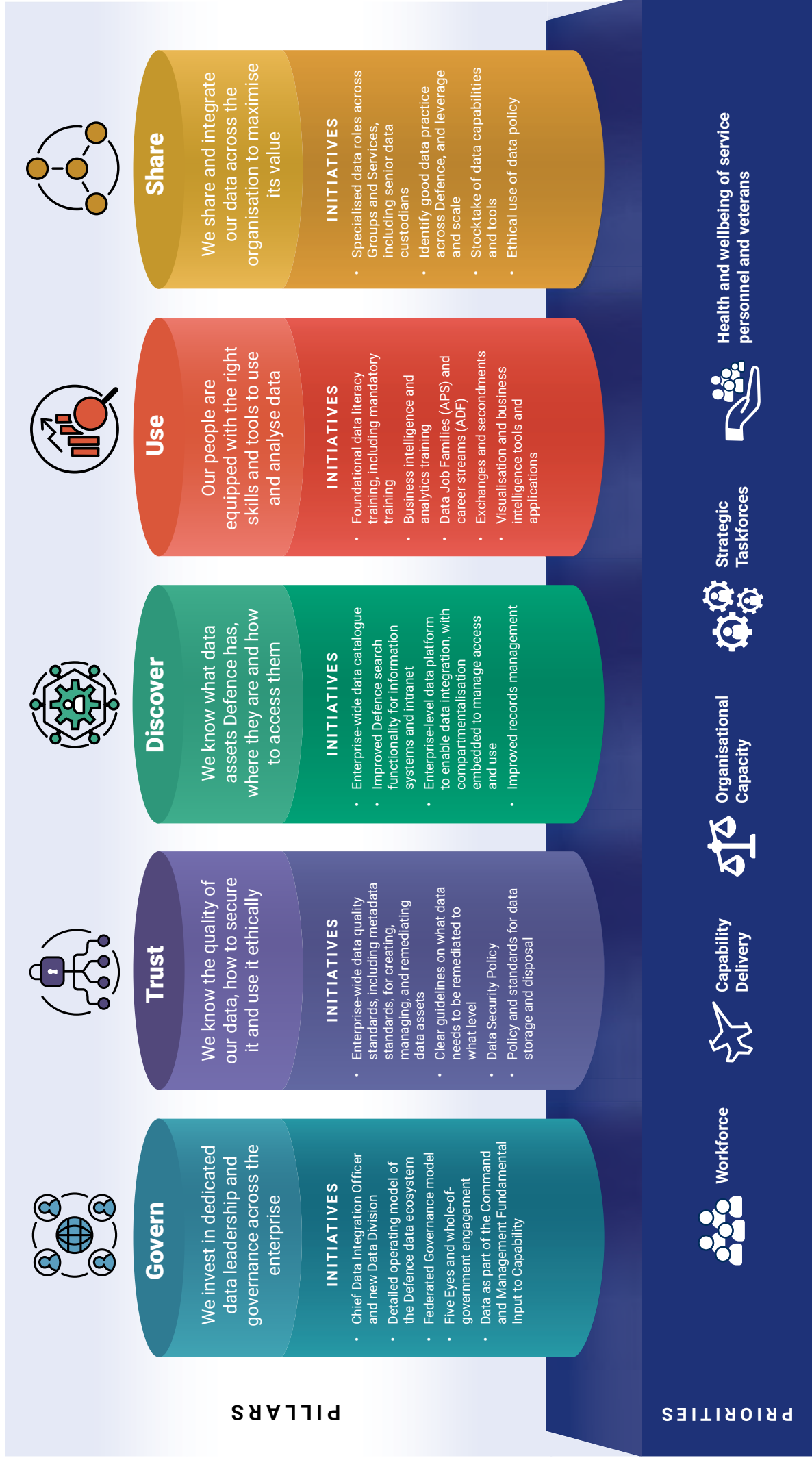
- Mission and operational data;
- Intelligence data;
- Capability development and management data, including portfolio, program, and project and product management;
- Corporate, human resources, and enabling services data;
- Cost management and finance data;
- Industry and economic data, including Australian defence industry and national shipbuilding;
- Science, technology, and research data;
- Strategy and policy data; and
- Engineering and logistics data.

We are not starting from a blank slate. We have pockets of excellence across the Defence enterprise. The *Defence Data Strategy* will connect these areas under a strategic framework to ensure we continue to develop skilled people, equipped with the right information, in order to make good decisions.

Defence Data Strategy 2021–2023

The *Defence Data Strategy* sets out the vision, five pillars, practical initiatives and priority data areas to lift our data maturity, embed data literacy as a cultural norm and put useful and trusted information at the centre of everything we do to deliver the Defence Mission.

Vision: Defence's data is a strategic asset – we value it, protect it and leverage it for strategic and operational advantage





Australia's changing strategic environment: through a data lens



The *2020 Defence Strategic Update* highlights that Australia is at the centre of an increasingly dynamic strategic environment. This environment is challenging Defence's ability to maintain a regional capability edge in advanced warfighting and enabling capabilities.

At the same time, the world is experiencing rapid levels of digitisation and exponential growth in the creation of data. The increasing connectivity of services and infrastructure to the internet will expose vulnerabilities in global supply chains, critical infrastructure and support services. These have the potential to be key targets in grey-zone activities as well as in conventional conflict.

Emerging and disruptive technologies, highly dependent on data, are being rapidly translated into weapons systems. Advanced technologies, such as artificial intelligence, robotics, and autonomous systems, will reduce decision time and improve precision and lethality.

The *2020 Force Structure Plan* outlines an ambitious capability program to respond to these changing strategic circumstances. This capability plan is providing the Australian Defence Force with the capability required to project military power in our region and beyond.

Lead the Way: Defence Transformation Strategy, announced in November 2020, outlined the necessity for Defence to be more agile and adaptive. We must continuously transform the organisation to ensure we can respond to any contingency regardless of the source, nature or scale.

Defence's ability to make connections and derive insights across diverse sources of data will underpin the successful adoption of the campaigning in competition approach our new security environment requires.

Lifting our data practices and leveraging our data holdings will be critical to **shape** Australia's strategic environment; **deter** actions against Australia's interests, and **respond** with credible military force when required. It will enable rapid well-informed decisions as the strategic environment and Australian Government priorities evolve. It will also provide a robust evidence base for effectively prioritising resources in the midst of changing circumstances.

A vision for Defence data in 2023

Through dedicated data leadership and governance, Defence will have implemented the foundational initiatives in the *Defence Data Strategy*. This will include:

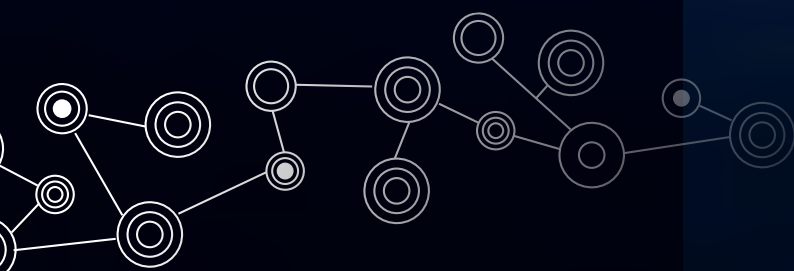
- Data-driven insights becoming an embedded part of our work.
- The ability to rate the quality of data assets, against gold, silver and bronze standards, so that our people automatically know the reliability of the data they are using.
- Information being delivered in the form of dashboards and visualisations, in preference to lengthy briefs.
- Defence working towards near real-time access to workforce and capacity data to drive agile resource prioritisation as priorities change.
- Defence being better equipped to capture, secure, understand, process, exploit and disseminate data to enable critical capability for the joint force spanning the Command and Control, Communications, Computers, Cyber, Intelligence, Surveillance, Reconnaissance, and Electronic Warfare (C5ISREW) sensor to effector spectrum.
- Defence increasingly documenting data assets through standardised metadata tagging, allowing personnel to search for and locate data from across the enterprise.
- Data management and workflow being increasingly automated, reducing the time and cost required to manually identify, cleanse and manipulate data.
- Visibility across inflight initiatives and key data and information assets, tools and systems to guide our technology investments.
- A range of options for data training and professionalisation, from foundational to advanced, being readily available and personnel equipped to treat data securely and ethically.
- Increased use of visualisations and business intelligence tools to inform decision-making, across all levels of Defence.

The importance of data in the battlespace

Command and Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance, or C5ISR, is the provision of timely and trusted information to support command decisions.

A wide variety of data is needed for Commanders to decide what actions to take to get a successful outcome. Commanders must understand:

- Their **troops**, how they are distributed geographically, what they are capable of doing, and for how long.
- The **terrain and sea states**, the geographical formations, and infrastructure to know how these will impact the movement and performance of troops, vehicles, planes and ships.
- The **weather** and its impact on the systems they use to detect and counter hostile forces.
- The status of their **supplies** – how much food and munitions they have and how long until they can be resupplied.
- The **enemy**, where they are, and what the enemy are likely to do, so they can determine how to defeat them.





The volume of data needed to make effective command decisions, across all these aspects, is increasing. Our ability to collect and distribute this data quickly will dictate the speed of our decision-making.

At the same time, emerging technologies, underpinned by data, are becoming part of our and our adversaries' capability. This is putting further pressure on the ability of Commanders to make fast, informed decisions.

As the speed of warfare increases, more decisions will need to be made autonomously as the volume of data outstrips the capacity of the human brain to process it.

The networks used to distribute data can also be attacked. Networks and data locations need to be carefully designed to ensure that informed and timely command decisions can be made even when the network is under attack.

Whether distilling large amounts of data using emerging data-driven technologies or securing our data the initiatives in the *Defence Data Strategy* set Defence up to deliver the right information on the right things at the right time to better support command decision-making.

Force Integration, Vice Chief of Defence Force-Executive

Our Partners

International

As part of our strong commitment to the Five Eyes alliance, we must ensure our approach to data management puts us in a position to be an effective and trusted ally and partner.

Defence's ability to securely manage and use data is a key determinant for Australia to successfully operate within the Five Eyes community.

Together, the Five Eyes nations are all investing in repositioning data as a strategic asset. As a community we are taking ownership of data and embedding the understanding that it has inherent, quantifiable value to our respective organisations, our partners, and our adversaries.

Aligning our data management and analytics approach with our international partners, where appropriate, will be important to maintaining our ability to work collaboratively and operate as part of a coalition.

Rapid and secure data sharing between people, platforms, and nations is at the heart of the US Defense's Joint All Domain Command and Control concept. Our investment in data maturity will ensure we can effectively operate under this construct when working in partnership with the United States.

New Zealand, Canadian, United States, Australian and United Kingdom Flags displayed at Buckley Air Force Base, Colorado, 2019. Photo Credit: Senior Airman Michael Mathews, US Air Force.

Australian Government

The Independent Review of the Australian Public Service recommended that all Australian Government agencies lift their digital and data practices. This will lead to better policy advice, regulation, and services for the Australian Government and the Australian people.

To assist agencies to improve data management practices, the Office of the National Data Commissioner released *The Foundational Four*. It guides agencies that are beginning their data journey to improve their data practices and build an organisational data culture.

The Foundational Four identifies the following key requirements for success:

- **Leadership:** A senior leader who is responsible and accountable for agency data;
- **Strategy:** A clear vision and plan for using data to achieve objectives;
- **Governance:** Established mechanisms to oversee data management; and
- **Asset Discovery:** Identified and recorded data assets.

The implementation of this inaugural *Defence Data Strategy* will enable Defence to deliver on all of these requirements. It also forms part of Defence's contribution to the forthcoming *Australian Data Strategy*.

Australian Defence Industry

Defence has established strong partnerships with Australia's growing defence industry. This is essential to our national security and to building a strong and resilient economy.

Defence's commitment to lifting our data maturity will have multiple benefits for these partnerships including:

- Providing greater value for money to Defence and reducing the cost to industry in competing for service delivery;
- Improving the design and delivery of the capabilities Defence requires to manage Australia's strategic challenges; and
- Signalling to industry the specialist skills required to develop innovative solutions for new capabilities.



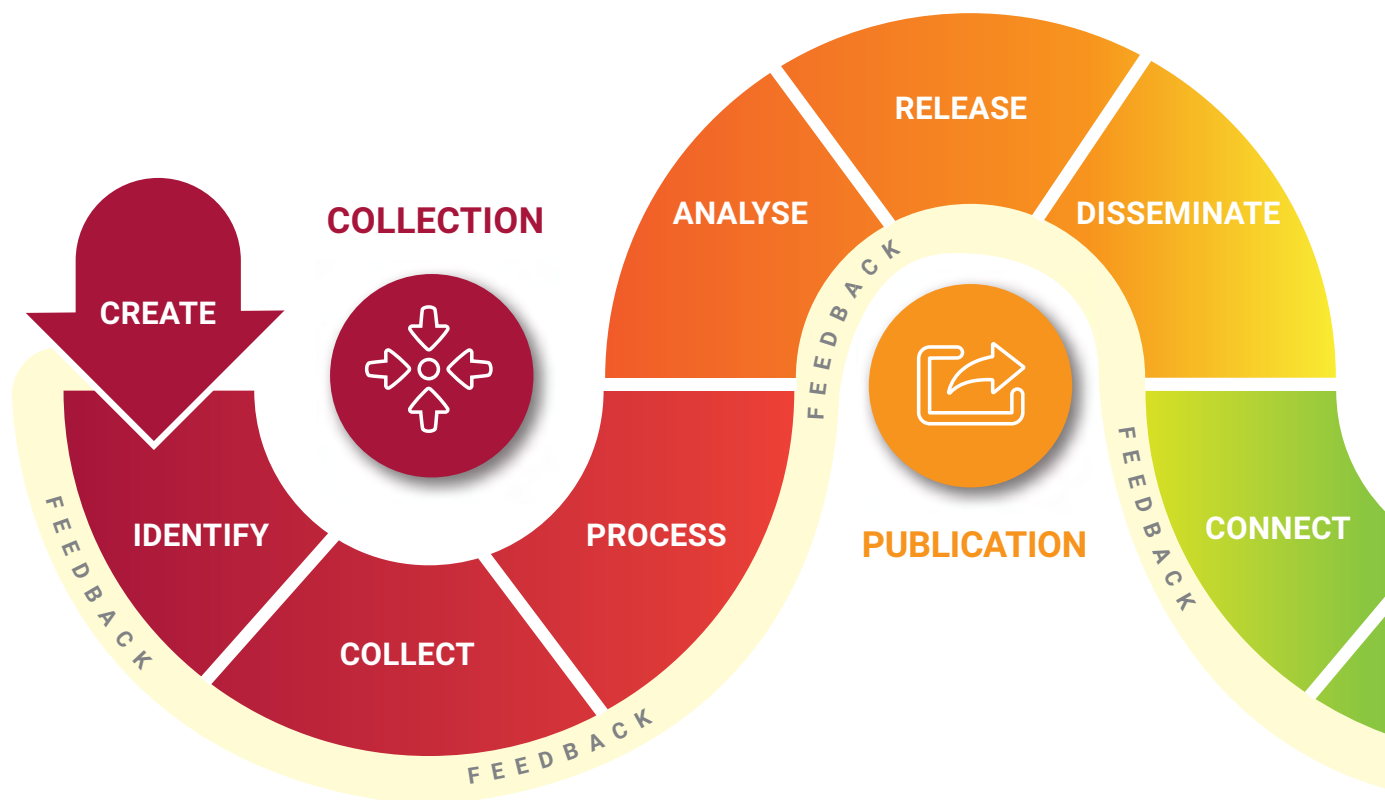
What is data?

Defining data

Facts represented as text, numbers, graphics, images, sound or video. Data is the raw material used to represent information, or from which information can be derived.

Some data is easily recognisable – administrative data, numbers in a spreadsheet, dates in a table. Some data is less recognisable such as emails, surveys, audio files, videos, photographs, maps, documents and reports.

Today data and information are becoming interchangeable terms. Instead, data and information are distinguished by the form that they take, such as structured or unstructured, and digitised or physical.



The data value chain

The data value chain above illustrates the evolution of data from creation through to disposal.

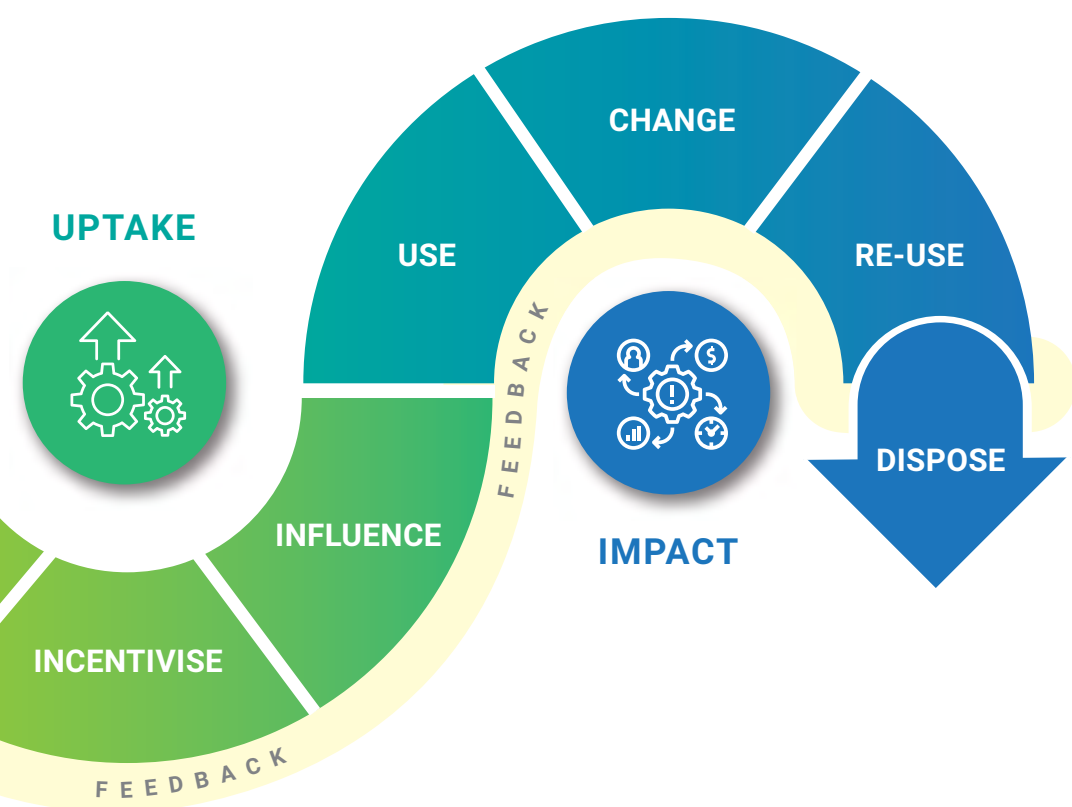
Throughout the process, from one end of the value chain to the other and back again, there should be constant feedback between data and analytics producers and consumers

The value chain outlines the process of how our data becomes valuable knowledge and insights to support Defence objectives.

The growth in data

In 2018, the total amount of data created, captured, copied and consumed in the world was 33 zettabytes (ZB) – the equivalent of 33 trillion gigabytes. This grew to 59ZB in 2020 and is predicted to reach 175ZB by 2025.

As a Defence example, we captured 15 terabytes (TB) of hydrographic data alone in 2018 and are expected to collect 255TB in 2025.



Our Data Challenge



Defence faces many challenges in lifting its data maturity.

We are a large, diverse organisation that undertakes many different functions, from the warfighter to the policy officer to the industry service provider in the regions. Due to Defence's size and diversity we could easily take a view that enterprise-wide data coordination and management is too hard and too complex, and will not deliver real benefits. However, to truly leverage the potential of our data assets and exploit the opportunities it presents, we require the ability to access data across the Whole-of-Defence.

Defence's current approach to data management is fragmented. With good intent, Groups and Services have been pursuing independent approaches to data management in the absence of dedicated enterprise-level leadership and governance.

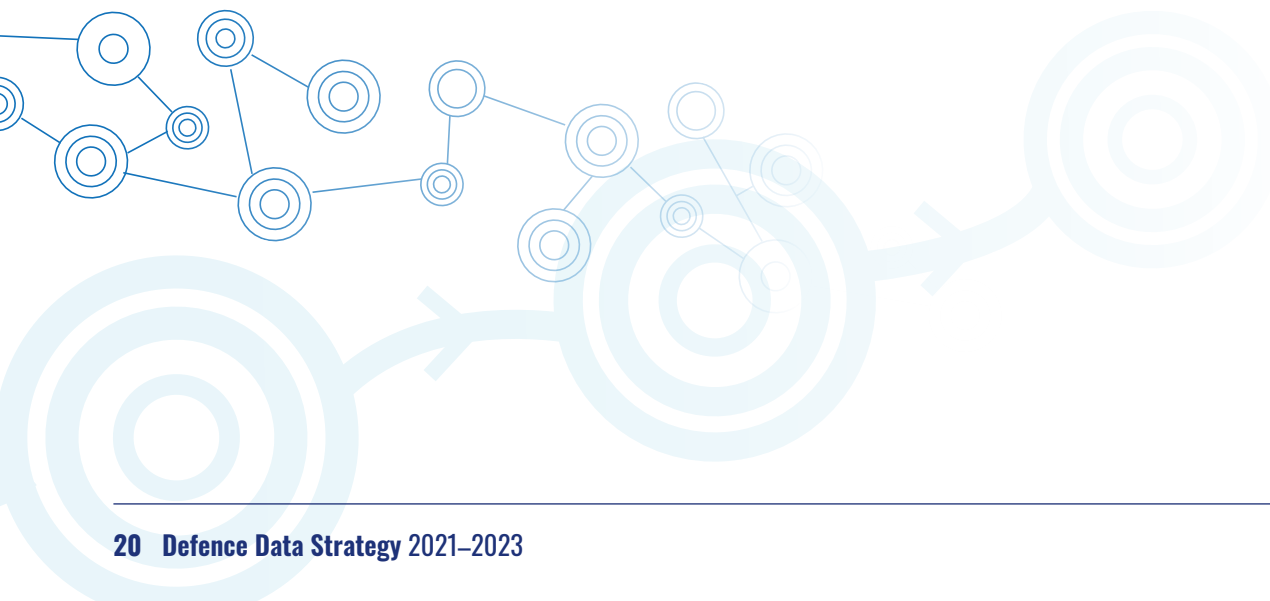
This has resulted in the development of ad hoc standards, policies, and practices, and a narrow focus on technology-driven solutions. It has also sometimes manifested in an unwillingness to share data across Groups and Services and a lack of trust outside our immediate work area.

The absence of a Defence-wide approach to data management and sharing has limited our capacity to know what data we hold, where it is, how to access it and whether it is of sufficient quality to provide a reliable evidence base for decisions. This has unfortunately led to large volumes of data being collected that may be of negligible value, cannot be reused, is often duplicated and is stored insecurely.

We also face challenges in:

- Not being aligned with Australian Government, Five Eyes and best practice standards;
- Low data literacy;
- Achieving an appropriate data workforce balance of public service, defence force and industry personnel; and
- An inability to search across the enterprise for data assets.

While acknowledging that there are discrete areas with good practice, collectively these issues have contributed to an immature data culture within Defence.



Our Data Maturity

In developing the *Defence Data Strategy*, a data maturity baseline assessment was undertaken through three surveys that engaged the:

- Senior Leadership Group;
- Technical Workforce; and
- Whole-of-Defence enterprise.

The three data maturity surveys provided responses from nearly 4,000 people across every Group and Service, from E01 (Private equivalent) to Senior Executive Service Band 3 and Three Star officers. The survey outcomes provided rich insights into Defence's data challenges and opportunities, and helped to form a measurable data maturity baseline for the organisation.

The surveys identified that failure to address Defence's low maturity will increase the risk of skilled data literate people leaving Defence. It is also likely to deter prospective employees from joining Defence – including data specialists and those with university qualifications who identified that their skills were going unused.

A total of 731 respondents to the Whole-of-Defence survey identified as having university or advanced qualifications in data. Of these, 334 were public service personnel and 258 were Australian Defence Force personnel. A total of 1,298 personnel identified that they would stay with Defence longer if it had mature data management and analytics tools.

The data maturity surveys confirmed that Defence has an overall low level of data maturity, with some pockets of excellence. It also identified that people across the organisation want to use data in a more sophisticated manner and are passionate about the opportunity to move into data-centric roles.

Defence works with emergency services personnel to input data into an integrated bushfire tracking system, 2019.
Photo Credit: Corporal Craig Bennet.



Increasing air time by harnessing data

Aircraft maintenance planning is a highly complex task. The integrated nature of modern aircraft maintenance policies means planning teams require a wide variety of data from multiple sources to make sure aircrafts are being serviced as efficiently and effectively as possible.

The success of maintenance scheduling directly impacts on Air Force's ability to make sure there are a sufficient number of aircraft available for operations at all times – also referred to as the *daily minimum*. The accuracy of the data, the capacity of planning personnel to comprehend and respond to changing circumstances and resource availability make this a difficult and time-consuming activity.

Simple planning tools, such as spreadsheets, are not sufficient to deliver results within this complex environment and, in the past, has led to sub-optimal fleet availability.

Given the large investment the Australian Government has made in our cutting edge fleets, Air Force recognised the opportunity to use data holdings to improve this activity.

To work towards a better outcome, Logistics Branch, Air Force engaged the Defence Science and Technology Group to develop a fleet optimisation model using advanced data analytics on an Air Force fleet. The C-130J was the trial aircraft.



An Australian Air Force C-130J Hercules aircraft, 2021.
Photo Credit: LSIS Richard Cordell.

Two separate maintenance planning models were developed. One model was designed for life-of-type fleet management considerations. The other model was designed to provide the maintenance unit with an optimised short term forecast. To assess the potential benefits of the two models, each one was compared to plans that were already in place for the C-130J.

The optimisation model increased average aircraft availability over the remaining fleet life by just over one per cent and prevented aircraft availability dropping below the *daily minimum*. This was not achievable in the original C-130J Fleet Plan. The short term planning model was used to test a range of scheduling scenarios for a known modification program on the C-130J, with modelling showing overall availability would be more than five per cent higher.

These availability improvements may appear small, however, the increase in fleet availability equates to hundreds of days and it has the potential to be rolled out across all Australian Defence Force aviation fleets – most likely yielding similar results.

Increased fleet availability provides greater surety in meeting the operational and training obligations for all aviation fleets and improves Defence's ability to **shape, deter** and **respond**. This is an apt demonstration of the capability benefits that may be achieved simply through the better use of existing data holdings. A second fleet will be modelled in 2021-2022 leveraging the statistical models developed for the C-130J trial.

Logistics Branch, Air Force



PILLARS



1. Govern



We invest in dedicated data leadership and governance across the enterprise

Data leadership and governance enables an organisation to manage data effectively and to a high standard throughout its lifecycle. It ensures data is managed in line with enterprise-wide policies and procedures, and that all personnel within the organisation understand and practice their responsibilities. This includes establishing processes to ensure data availability, usability, consistency, integrity and security.

Leadership

A data-driven culture requires passionate and dedicated leadership who commit to delivering avenues and opportunities for everyone.

To set the foundations for an uplift in Defence's data maturity, a Chief Data Integration Officer will be established at the centre of the enterprise. They will be responsible for embedding strong data governance and management to achieve our strategic objectives.

The Chief Data Integration Officer will be accountable for delivering the *Defence Data Strategy* initiatives, driving cultural change around data, and supporting Defence to become a more data-informed organisation. They will be the job family owner for new data-centric roles and professionalisation programs for public servants, military and industry personnel.

The appointment of a Chief Data Integration Officer does not negate the crucial data leadership role performed by all levels across the organisation. The role, instead, provides a central point of leadership to coordinate and focus data initiatives and governance.

- **1.1** Establish a Chief Data Integration Officer, accountable to the diarchy, through the Associate Secretary and the Vice Chief of the Defence Force. The Chief Data Integration Officer will lead the uplift of Defence data, implement the *Defence Data Strategy* initiatives and be accountable for enterprise data management.
- **1.2** Establish supporting functions under the Chief Data Integration Officer for data governance, assurance, security, policy, standards, professionalisation, literacy, analytics and visualisation. These functions will include teams that can deploy to areas across Defence to support data management requirements.
- **1.3** Develop a detailed implementation plan for all *Defence Data Strategy* initiatives and priority data areas.
- **1.4** Develop the Defence Data Operating Model, including baselining the current data ecosystem, establishing a target future state, and creating a pragmatic roadmap to transition between them.



Governance

Disciplined data governance aligned to Defence's Mission will deliver strategic and operational advantage.

Strong data governance will give Defence the ability to prioritise data investments and align them with organisational and user needs. It will enable good data management practice aligned with our Australian Government, Five Eyes and industry partners and facilitate the sharing of lessons across these communities.

A new federated governance model, supported by appropriate policies and guidance, will be implemented to support these outcomes. The Data Management Body of Knowledge (the international data standard) identifies that federated governance models are most effective for large, complex organisations.

What is a federated data governance model in Defence?

A federated data governance model allows the Chief Data Integration Officer to develop and release enterprise-wide guidance, with appointed data custodians executing and implementing this at the Group and Service level.

This federated governance model will align the *Defence Data Strategy* and accompanying policies, frameworks, and services with activities across the enterprise. This will ensure the needs of different parts of the organisation can be met by the people who understand them best. It will promote the sharing and integration of data assets across Defence to support enterprise requirements and empower Group and Service data functions.

A new Defence Data Management Board will be established to coordinate and prioritise data management activities. Chaired by the Chief Data Integration Officer, the Defence Data Management Board will bring together senior Data Custodians to ensure areas are connected and sharing expertise. The Board will report through the Enterprise Business Committee, and to the Investment and Defence Committees, if required.

- **1.5** Establish the Defence Data Management Board and appoint appropriate Defence Senior Executive Service Band 2 and Australian Defence Force Two Star representatives as Senior Data Custodians.
- **1.6** The Chief Data Integration Officer will lead Defence engagement with Australian Government and Five Eyes data and analytics forums. This will include a review of current Defence participation and a realignment to ensure the organisation is actively engaged at the right level across all key forums.






A soldier using the Vulcan Oil Condition Monitoring dashboard at the Army School of Electrical and Mechanical Engineering, 2021. Photo Credit: Nick Draper.

Using our data to support Australian soldiers

Australian soldiers rely on access to the best possible technology to complete their mission, whether it be training in Australia or deployed on operations. The Land Engineering Agency has been supporting Australian soldiers for over 80 years by providing dedicated engineering services throughout the land materiel capability lifecycle.

Developed by the Land Engineering Agency, Capability Acquisition and Sustainment Group, Vulcan is a data engineering and analytics capability that leverages Defence's strategic data assets to improve mission success, both now and into the future. This is exemplified by the Vulcan Oil Condition Monitoring framework which integrates datasets received from armoured vehicle components, such as engines and gearboxes, usage history and maintenance records to evaluate the condition of equipment and to automate maintenance actions.

The introduction of this framework provides multiple benefits to our soldiers.



Soldiers gain increased availability to equipment by eliminating unnecessary maintenance activities. Simultaneously, regular monitoring improves reliability through early detection and prevention of failures that could put an operation at risk.

Defence is saving millions of dollars in maintenance costs by using data, such as oil sample analysis and sensor readings, collected from vehicle components to determine when to service equipment, rather than depending on fixed servicing intervals.

As data volumes increase over time the automation of data flows has become essential.

These automations include:

- Ability to enter usage and condition metrics directly into the Defence logistics information system, enabling soldiers to devote more time to their primary tasking;
- An automated email service to notify the relevant maintenance authority when action is required on vehicles; and
- A Defence web service enabling the automated transmission of oil analysis results from an external laboratory to a central location within the Defence Protected Network Environment.

The Vulcan Oil Condition Monitoring framework demonstrates how complex technical datasets can be transformed into insights to enable informed decision-making for soldiers.

These insights could only be achieved by establishing foundational data management practices. The initiatives in the *Defence Data Strategy* are the foundational steps that Defence will take to establish good data management practices that enable us to exploit the numerous datasets across our enterprise.

Land Engineering Agency, Capability Acquisition and Sustainment Group

Data as a Fundamental Input to Capability

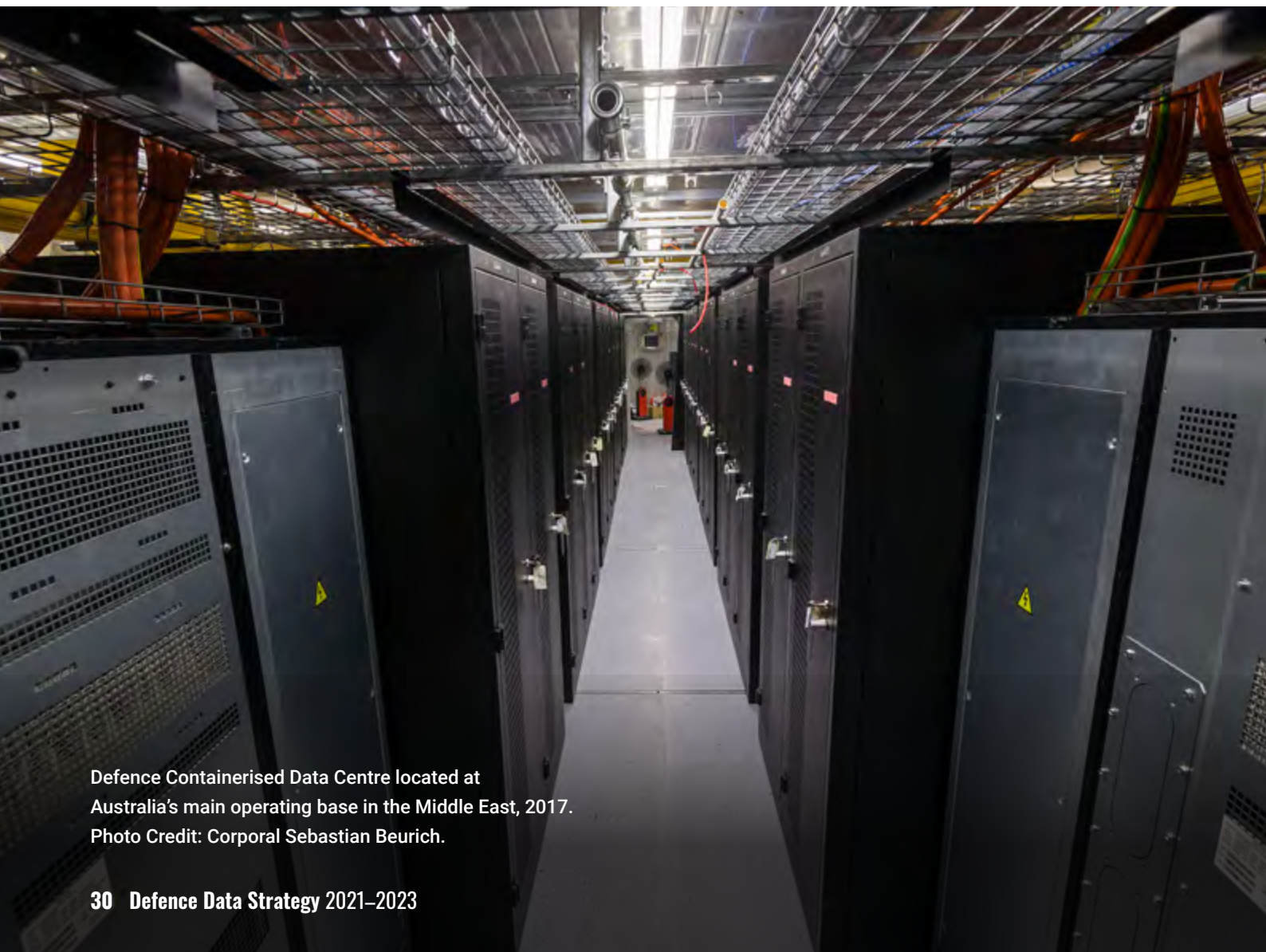
Increasingly, Defence capability has significant data dependencies. Capabilities require large data inputs and the capacity to share data across multiple platforms. They also produce large amounts of data that needs to be managed, stored, secured and, if appropriate, reused. The centrality of data and information to warfighting, and especially next-generation capabilities, has markedly increased the importance of data as a fundamental input to capability.

However, experience has shown that data requirements are often not considered in the initial design and development of capability. We often have to retro-fit these requirements, creating a number of additional challenges, costs and risks, resulting in missed opportunities for joint collaboration and efficiency.

Fundamental Inputs to Capability provide a checklist designed to report on all inputs that enable the effective and ongoing generation of Defence capability.

Incorporating data into the Fundamental Inputs to Capability model will ensure that requirements are identified early, factored into the planning process and considered across the capability lifecycle.

- **1.7** Incorporate Data into the Command and Management Fundamental Inputs to Capability. This will enable Capability Managers to consider the data requirements necessary to deliver optimal capability outcomes and factor these into capability projects and programs at the design stage.



Defence Containerised Data Centre located at Australia's main operating base in the Middle East, 2017.
Photo Credit: Corporal Sebastian Beurich.

2. Trust



We know the quality of our data, how to secure it and use it ethically

Trust takes time and commitment – establishing trust in data is no different. For organisations to trust their use of data it requires standardisation and regular assurance. It also requires a trained workforce, proficient in maintaining privacy, ethical and security considerations.

Standards and assurance

Defence needs to know that the data we use as a basis for making operational decisions, advising senior decision-makers or delivering services is accurate and timely.

What is metadata?

Metadata literally means *data about data*. It describes the characteristics of data and is used to improve an organisation's understanding of data and data-related processes.

The accuracy of targeting data is critical and will require higher levels of regulation and assurance. By comparison, an operational intelligence picture requires more agile use of data and is often based on the best information available at the time. This data may require less regulation and assurance. Internal or corporate data may be based on indicative or rough order of magnitude estimates.

Defence will develop enterprise-wide quality standards, with a particular focus on providing guidelines on metadata standards. This will allow for improved discoverability of critical data and integration of datasets. It will create the conditions for automation as datasets become machine-readable and discoverable.

What are Gold, Silver, and Bronze certificates?

The quality rating applied to a dataset which is assessed based on the data's source, origin and platform.



Gold: thoroughly examined and considered fit for general release and re-use, including public and government level release.

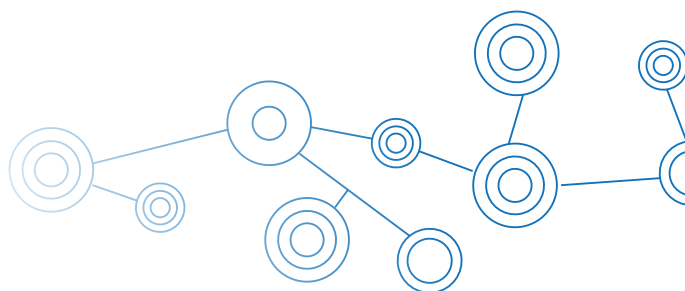


Silver: considered *fit for purpose* for a specific business use case and for specific user requirements, but generally not to be re-used or released publically.



Bronze: discoverable and has assigned custodianship, but with only a basic assessment of its quality.

Assuring our data will allow for an assessment of which datasets are required to be at what level of quality. Defence will adopt the Gold, Silver, Bronze data rating system in line with best practice. This will meet the requirements of the enterprise and empower our personnel to make informed decisions with confidence.



- **2.1** Establish enterprise-wide data quality standards, including metadata standards, for creating, managing, and remediating data assets. Develop guidelines for different types of datasets, consistent with Defence requirements and Australian Government standards.
- **2.2** To meet the requirements of the Defence enterprise, determine which datasets need to be assured to what level.
- **2.3** Include the quality rating of the data used on dashboards and reports, where possible, so that users know the level of assurance applied to the datasets used.

Security and privacy

Defence is the custodian of incredibly sensitive data, whether it be national security-related or information about our personnel. The increase in grey-zone activities, including cyber attacks, and foreign interference, requires a renewed focus on our data security and storage processes. However, we need to carefully manage the inherent tension between the need to discover and use data and ensuring that appropriate security and privacy requirements are met. This requires the adoption of a risk-based approach to data security.

A risk-based approach means asking:

Is the risk of sharing data and insights greater than the risk of not sharing, and potentially, having decisions made based on incomplete information?

To help personnel navigate this context, Defence will deliver a Data Security Policy. The Policy will outline the correct procedures for handling and storing all types of Defence data and provide a framework for navigating the risk-based approach.

- **2.4** Deliver a Data Security Policy to communicate to Defence personnel the importance of using and storing data in a secure and risk-based manner.
- **2.5** Consistent with Australian Government obligations, establish policy and standards for data storage and disposal supported by appropriate systems and tools.



Royal Australian Navy MH-60R Seahawk helicopter departs HMAS Adelaide during Operation Bushfire Assist, 2020.
Photo Credit: ABIS Thomas Sawtell.

Metadata matters

Army has a long history of confronting its adversary and completing the mission.

In 2020, the adversary took a very different form. Major crises, including bushfires and the COVID pandemic, required Army to re-think how to respond.

Confronted with this new adversary, there was a hunger for fast, credible, relevant and actionable information to support operational planning.

The Army Knowledge Centre harnessed information from across its databases to support the rapid provision of knowledge to decision-makers. The Centre was able to do this through the design of data structures and well-developed metadata standards that allowed information to be tagged. These tags enabled searching by key words and themes across linked datasets.

Although the threat was different, planning at the start of these operations still needed to consider tasking against relatively common lines of military effort. As the knowledge curated by the Centre is structured around a schema for missions and planning considerations, extracting relevant lessons into a concise report to meet Commanders needs at multiple levels was rapid.

Foundational metadata standards built into the database, facilitated the rapid generation of products for operational planners that drew connections between key themes associated with the mission and the prescribed tasks.

Defence has the potential to realise similar benefits across the enterprise. The foundational initiatives in the *Defence Data Strategy*, in particular, cataloguing data assets, implementing metadata standards, and improving discoverability, will support our information management and knowledge application needs into the future.

Knowledge Management Centre, Army

3. Discover



We know what data assets Defence has, where they are and how to access them

Harnessing the value of data can only be achieved if all personnel know what data assets exist and how to access them. The ability to discover and access data creates an organisational mindset where, no matter what your role or task, it is done with all the relevant data and information available.

Data asset identification and discoverability

In Defence, we deliver advice to many stakeholders including ministers, industry, and international partners. We deliver services to meet a range of needs and undertake operations both domestically and internationally. Our ability to provide clear, timely, and consistent advice, high-quality services and achieve operational decision superiority is dependent on the discoverability of our data assets.

When data remains in silos and is undiscoverable or inaccessible it only serves the needs of a limited area of the organisation. It restricts the development of new insights and views that are produced by combining datasets in different ways to identify patterns and drives poor data security practices.

Defence will take an enterprise approach to increasing the discoverability and accessibility of our data holdings through:

- Cataloguing important data assets;
- Improving our ability to search for data; and
- Implementing the right systems, platforms and tools to deliver on our data usage needs.

What is a data asset?

A data asset is any electronic data that exists in computer systems. Data assets include a system or application output file, database, document or web page.

What is a data catalogue?

A data catalogue is a detailed inventory of all data assets in an organisation that uses metadata to help manage those assets. It supports the collection and organisation of data assets, and improves discoverability and access.

Why is this important?

Without a data catalogue we look for data by sorting through documentation, talking to colleagues, or working with familiar datasets. With a data catalogue we are able to search and find data quickly, see all the available datasets, evaluate and make informed choices about what data to use and perform quality analysis efficiently.

We spend less time searching for data and more time conducting analysis and producing insights and evidence.

- **3.1** Establish and maintain an enterprise-wide data catalogue where Defence personnel will be able to search for and locate data, dashboards and visualisations for their specific needs.
- **3.2** Review the search functionality of Defence's information systems and intranet to improve the ability to access relevant data and information in a timely manner.
- **3.3** Establish an enterprise-level data platform to enable data integration, with compartmentalisation embedded to manage access and use across specialised areas and security levels.



Sergeant Thomas Lane, Avionics Technician at No. 36 Squadron, uses the HoloLens mixed reality device during C-17A Globemaster maintenance.

Data fuels artificial intelligence

Artificial intelligence will play a vital role in Defence's future operating environment. This emerging technology will be critical to delivering on our strategic objectives of **shape, deter** and **respond**. Maintaining a capable, agile and potent Australian Defence Force is becoming increasingly dependent on artificial intelligence technologies.

What is not so well understood is that for Defence to harness the opportunities presented by rapidly advancing artificial intelligence technologies, our data holdings must be managed and discoverable in a way that supports the development of artificial intelligence tools. These tools must be able to leverage Defence's data to operate at their full potential.

Defence is taking steps to prepare for this future.

Defence has established the *Defence Artificial Intelligence Centre* in the Joint Capabilities Group. It will accelerate our capability foundations and the understanding and implementation of coordinated artificial intelligence technologies across the enterprise.

Joint Capabilities Group, in partnership with the Chief Information Office and Defence Science and Technology, has established the *Defence Technology Acceleration Collaboration Laboratory*. It will connect Defence with academic and industry expertise. Harnessing a multi-cloud environment the laboratory is testing prototypes to solve capability challenges and inform future capabilities.

Defence Artificial Intelligence Centre, Joint Capabilities Group

Document and content management

Document and content management is a key component of data management. It covers the capture, storage, access and use of data and information stored outside relational databases.

As we move to an increased focus on digitisation, Defence is creating and collecting more records than ever before. As at June 2021, an average of 6.2 million documents were being captured by the enterprise each month.

Defence has legislated responsibilities to create, manage, preserve and retain information in order to meet the provisions of the *Archives Act 1983* and accountability to the Australian Government and the Australian people.

Continuing to improve how Defence creates, manages and uses its information and data will require an ongoing emphasis on governance, capability building and reducing areas of information management inefficiency and risk.

We need to focus on how we manage our content by determining what capability best supports the collection, discoverability, access, and disposal of our records.

We also need to develop a strong understanding of the importance of effective records management in our personnel. Our people need to understand how to undertake records management and why it matters. Developing a library of simple and clear factsheets and guides will better support our people and strengthen our records management practice.

- **3.4** Implement improvements to Defence's record management practices and ensure Defence delivers on its legislative obligations.
- **3.5** Develop a library of simple, clear, and easily accessible fact sheets and guides on records management. These products should be system agnostic wherever possible.

Getting the data channels right in Navy

In order to produce better mapping and measurement inputs for the Defence Corporate Plan and Enterprise Risks process, Navy has developed a strategic performance and risk management system. This system maps key activities and deliverables that identify and scope mitigation activities and assurance functions. With the subsequent development of a quantitative measurement system to support decision-making by Chief of Navy's Strategic Advisory Council we have undertaken a back to first principles review of data streams within Navy - where they go and what they are used for.

Navy's vision is to use existing data and information systems from across the Service and the Defence enterprise to inform business performance reporting, rather than implementing another set of adjacent Navy specific reporting processes that would result in productivity and efficiency costs to personnel.

Conceptually, this is intuitive and straightforward. In reality we double or triple handle data using disparate and unintegrated systems. This has been driven by iterative development, as well as the highly deployable and agile nature of maritime platforms and their management across all fundamental inputs to capability.

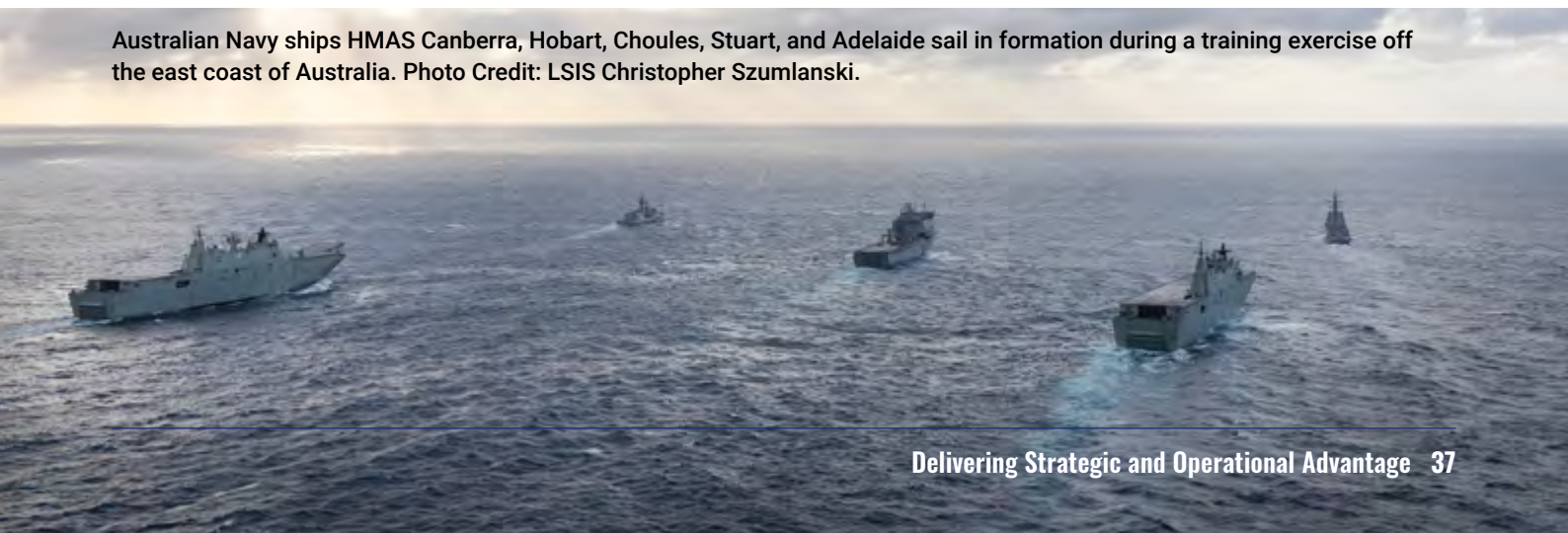
This quiet revolution in data usage is seeing the creation and deployment of data pipelines direct from existing applications and systems into central awareness tools from which decisions can be made and appropriate resources allocated.

In time, this will include direct input from established systems, including PMKeyS, the Capability Development Management and Reporting Tool, and Smart Owner. While the implementation of this quantitative based system is being introduced iteratively across the Five Navy outputs, there has already been observable improvements in the timeliness of assessments.

The continued refinement and adjustment of this information system, enhanced through greater consistency in datasets to enable increased utilisation of automated bot processes, will continue to enhance decision-making within Navy. It will also increase Navy's understanding and tracking of strategic outputs for the wider Defence enterprise.

Navy Headquarters, Navy

Australian Navy ships HMAS Canberra, Hobart, Choules, Stuart, and Adelaide sail in formation during a training exercise off the east coast of Australia. Photo Credit: LSIS Christopher Szumlanski.



4. Use

Our people are equipped with the right skills and tools to use and analyse data

As all organisations transition to an increasingly digitised world, they are investing in the data and digital capabilities of their people. This is done with the knowledge that the unprecedented growth and untapped potential in data holdings is only going to continue. This investment provides personnel with the skillsets to exploit data, held within an organisation with partners and publicly, to gain advantage and remain relevant in a changing environment.

Data literacy

As outlined in *Lead the Way: Defence Transformation Strategy*, Defence needs to build a skilled and flexible workforce in order to meet the challenges of the future. This includes supporting and equipping all our personnel with the right skills to maximise the use of our data. Investing in the data skills of our people is how we will set the right conditions for thriving in our strategic environment.

Continual education of our people in the use of data will be essential to remaining a competitive fighting force. It is also critical to evidence-based decision-making.

We will train our people to share, analyse and leverage data across the organisation in a secure and ethical manner, in order to drive a collective lift in our data capability.

- **4.1** Consistent with Defence's future focused capabilities, build and implement mandatory foundational data literacy training, accessible to all Groups and Services, to provide personnel with baseline data skills, including data hygiene, security, privacy and ethical use of data.

Data professionalisation

Defence will become a leader in developing data specialists, and in supporting those with a passion for using data in their daily work.

We will invest in our specialist data practitioners and support their careers through learning and professionalisation pathways. This will attract and retain the best available talent in Defence and within the broader national security community.

The creation of data career pathways for our integrated workforce will ensure we can identify and invest in our data specialists. This will provide meaningful career options and development opportunities. It will also support the upskilling and retraining of existing personnel looking to transition into a data-focused career or increase data usage in their current roles.

- **4.2** Develop a data training continuum, from introductory courses through to micro credentialing and advanced degree programs.
- **4.3** Explore the feasibility of developing data specialist career streams for the Australian Defence Force, with an initial focus on information warfare and cyber.
- **4.4** Leverage the Australian Government data professionalisation initiative and integrate learnings into Defence, including the establishment of data job families for Data Analysts, Data Scientists, and Data Engineers.
- **4.5** Develop opportunities for exchanges and secondments across the Australian Government, Five Eyes nations and industry to strengthen data skillsets through on-the-job learning and knowledge transfer.

Data analytics and visualisations

The value of data is realised when it is transformed into information, insights and, ultimately, decisions and actions. To do this, Defence needs to be able to distil a lot of data easily – whether it be in the office, on training exercises, or in the battlespace. We must empower people across the enterprise to easily and quickly consume information, and make better, more informed decisions.

To achieve this, Defence will provide our people with the necessary training and tools to transform our data into valuable and influential insights. We will equip our people with the skills to understand, develop, and communicate using data visualisations and dashboards.

- **4.6** Through the stocktake of data capabilities and tools, understand what visualisation and business intelligence tools and applications best support our people and make them available for use across Defence.
- **4.7** Provide training to Defence personnel to understand how to analyse data and create visualisations, and communicate using these products for better decision-making.

Harnessing data to improve supply chain network resilience and enabling Australian sovereign capabilities

The security and resilience of Australian sovereign capabilities are of paramount importance to Defence.

Defence's supply chains are globalised with complex assembly components manufactured by companies located across a number of different countries with differing geopolitical influence levels. From both a security and resilience perspective, Defence seeks to understand its supply chains to ensure a continuity of supply.

The Capability Acquisition and Sustainment Group is making significant inroads into understanding Defence supply chains. This will be enhanced by the establishment of the Defence Supply Network Analysis Program, to be delivered by the end of 2021.

What is SNAP?



Mapping

Big data analytics and augmented intelligence are leveraged to analyse surface and deep web data sources to build Supplier Network maps and identify opportunities and exposures



SNAP Methodology

The Supply Network Analysis Program (SNAP) has developed a repeatable and scalable methodology to translate mapped opportunities and exposures into tangible benefits



Benefit Workstreams

The SNAP Methodology is applied across six interdependent workstreams to focus outcomes into areas of tactical and strategic importance



The Program will use Open Source intelligence data collection, accelerated by machine learning and data-driven analytics, to map and identify opportunities and potential risk exposures in our supply networks.

Through this Program, and in line with the *Defence Data Strategy*, Capability Acquisition and Sustainment Group recognises the need for the organisation to move away from using data as a rear-view mirror and towards integrating analytics directly into our daily decision-making.

Beyond this, the Program will provide Defence visibility of its supply chains, making them more transparent across multiple tiers. By doing so, Defence will be better equipped to understand the specific risk lens that apply to our supply networks – be it financial, operational or geopolitical – and actively monitor red flags as they arise in real-time.

Supply Network Analysis Program, Capability Acquisition and Sustainment Group

5. Share

We share and integrate our data across the organisation to maximise its value

Organisations that have built a data culture around sharing are better placed to respond to future challenges and opportunities. This is because data is used and re-used, through a collect once, use often approach, to solve different problems as they arise. It allows organisations to increase the speed of their insights by moving away from manual, siloed data practices.

Leveraging good data practice

A culture of sharing allows the Defence enterprise to harness untapped opportunities – whether that is combining datasets to develop new insights or leveraging good data practices.

There are pockets of innovative data practices all across the Defence enterprise – we will connect these dots and create a community. Sharing of expertise will lead to an enterprise-wide data uplift as we leverage good practice and scale up to the level we require.

- **5.1** Undertake a stocktake of data capabilities and tools to understand Defence's baseline capability and create a mechanism to identify good data practice and leverage and scale to an enterprise-level.

Establishing data custodians

Across Defence, we have traditionally held data assets within our immediate work area. We have also been at times reluctant to share more broadly. When we have shared, it is generally because of our personal networks, rather than through a systematic approach to accessing data. As a result, Defence is yet to fully realise the substantial benefits of the data assets we hold.

The establishment of data custodians across the Defence enterprise reinforces that no one person or area owns Defence's data. It is a Commonwealth asset and, with appropriate controls, should be accessible to personnel across the Defence enterprise who need the information.

Data custodians will be those who have primary responsibility for data within their Group, Service, Division, or Command. Data custodianship should be a core part of their daily work, rather than an additional responsibility.

There will, of course, be times when sharing Defence's data assets is not possible, for reasons such as security or privacy. This should not automatically result in a total restriction on access to that data, especially if it is of great value to achieving the Defence Mission. We need to be able to take a risk-based approach and ask whether the potential benefit, which may not yet be fully known and understood, outweighs the risk of sharing.

- **5.2** Establish data custodians at appropriate levels to support the governance, management, and sharing of data across Defence.

Ethical data

Ethical considerations are a key component of trusting our people to use data appropriately. These considerations range from collecting and managing sensitive and personalised data through to using and sharing it, potentially with the public.

Guidelines around the ethical use of data will be developed to ensure we have a shared understanding of our legislative and ethical responsibilities. This will support personnel to navigate these considerations when sharing and using sensitive data assets.

The guidelines will balance ethical data management with the requirement to use and reuse data if it can improve decision-making and Defence outcomes. The *Australian Code for the Responsible Conduct of Research* and the *National Statement on Ethical Conduct in Research* will inform these guidelines. The ethical use of data guidelines will form part of the *Defence Human and Animal Research Manual* and policies.

- **5.3** Deliver an ethical use of data policy, providing personnel with a framework to navigate managing sensitive data assets and insights across the data lifecycle.

Managing research data at scale

Research data is integral to Defence's capability edge. It plays a unique role in supporting innovation across all areas of Defence activity, beginning in the key research domains; science and technology, health and medicine, social science and humanities and strategy and policy.

Research data varies from operational data to business data. It can be very complex and diverse, potentially extremely large, and cover wide spans in terms of sensitivity, size, format, proprietary and experimental sources and security classification.

New ways of doing research are transforming how data is collected, manipulated, analysed and visualised. Research can now be done at scale, bringing together expert collaborative teams of researchers, combining data from different sources and employing cutting edge technologies to deliver new Defence insights and knowledge.

To take full advantage of the potential of research we must develop frameworks and initiatives for managing research data, aligned with the *Defence Data Strategy* pillars – Govern, Trust, Discover, Use, and Share.

The key considerations for managing data across the research lifecycle are:

- Research projects must have a Data Management Plan that details intended data collections, documentation, metadata, storage, accessibility, sharing protocols and legal and ethical compliance requirements for the project.
- Research data will be quality assured to the appropriate standard and secured to mitigate internal and external threats to privacy and unauthorised use.
- Research data must meet strategic, ethical and legal requirements, including that human research data is managed appropriately to protect the welfare and privacy of participants.

These key considerations affect the creation, collection, collation, aggregation and linkage, access controls, and reporting of Defence research data. Detailed Defence policy and guidance on the management of human research data is outlined in the *Human and Animal Research Manual*.

To maximise the value of data collected for research purposes, documented data should be shared together with discovery metadata, after conducting risk assessments that balance security and privacy requirements.

Defence Science and Technology Group and Defence People Group

PRIORITY DATA AREAS



Defence is a very large, complex organisation with vast data holdings and constantly shifting priorities.

To ensure we focus our effort in the right places, five priority data areas have been identified to drive Defence's data uplift over the next two years. All five areas address high priority questions facing the organisation where data and analytics can enhance decision-making. They also require the combining of datasets from across the enterprise, rather than from single domains. The Chief Data Integration Officer will drive the design and delivery of the five data priorities, in partnership with domain leads.

Workforce: What personnel do we have, where are they located, what do they do, and what skills do they have?

Determining how to best utilise our workforce requires a robust enterprise view of the whole of Defence workforce - Australian Defence Force, Australian Public Service, and industry.

Prioritising our workforce, adjusting rapidly as priorities change, and investing in future skills requires a near real-time view of our people. We also hold a duty of care to all personnel deployed across Australia and the globe. To exercise this responsibility fully we need to have a common picture of our personnel.

Bringing together data, analytics and automation will provide this understanding of our workforce profile: who we have, where they are located, what they do and what skills they have. Over the next two years we will prioritise the acceleration of workforce data management and analytics. Investment in workforce data management is an enduring commitment and this work will continue beyond the life of this initial Strategy.


Capability Delivery: Are we delivering the right capabilities at the right time?

The 2020 Force Structure Plan outlines a capability program of over \$270 billion over 10 years to respond to our changing strategic circumstances. Defence must be well positioned to understand how it is delivering against the *Force Structure Plan* and whether that Plan will deliver the capability effects required to meet our future strategic challenges. Defence is also required to provide the Australian Government and the Australian people, where appropriate, with answers to these questions.

Bringing together data, analytics and automation will provide better insights into capability delivery, help us understand if our projects and programs are on track to deliver the right capability effect, and support reprioritisation of the Integrated Investment Program when our strategic circumstances change.

Organisational Capacity: How do we better understand our organisational capacity and provide policy advice to Government on the impact of responding to new requirements and unplanned contingencies?

Government is increasingly asking far more of the Defence enterprise. This includes undertaking extended operations, responding to domestic emergencies, increasing our commitments in the region, and establishing strategic taskforces to address emerging priorities in new and unfamiliar ways. Over the last two years we have deployed more Australian Defence Force personnel, including Reservists, to national responses than we have in the last 10 years. A significant numbers of Defence public service personnel are also being deployed across Australian government agencies.




We are supporting the Australian Government in ways we have never done before, starting with the COVID pandemic response and continuing through the new public service surge workforce initiatives.

The capacity of Defence to maintain, and potentially increase, this new operating tempo needs to be better understood. Data and analytics will provide an evidence base to better manage capacity challenges and provide clear policy advice to the Australian Government on the organisation's ability to respond to new requirements, and potential adjustments that may be required.

Strategic Taskforces: How do we rapidly stand up strategic taskforces and support their unique data management needs?

Strategic taskforces are increasingly used as a mechanism to support Defence's role in responding to emerging temporary priorities. In the last 24 months Defence has created taskforces to respond to the 2019/2020 Black Summer Bushfires, the COVID pandemic, the Inspector-General of the Australian Defence Force Afghanistan Inquiry, and the Royal Commission into Defence and Veteran Suicide.

Establishing strategic taskforces requires an ability to quickly determine capability needs and understand which personnel across the enterprise are best suited to these roles. There is also a need to quickly understand the property and information technology requirements of the strategic taskforce. Once established, there are usually specific and unique data management processes that need to be established, including real-time data visualisation and historical records management. This priority data area will be a valuable resource as Defence continues to employ taskforces to address emerging issues.



Lifetime Wellbeing of Current and Former Serving ADF Members and their Families: How can we better support whole-of-life health, wellbeing and safety outcomes for current and former Australian Defence Force members and their families?

In response to the 2019 Productivity Commission's 'A Better Way to Support Veterans' Report (Recommendation 11.2), the Australian Government agreed that Defence and the Department of Veterans' Affairs would develop a joint Data Sharing and Analytics Solution, underpinned by complementary Wellbeing Frameworks.

The Data Sharing and Analytics Solution will link data on serving Australian Defence Force members with internal Defence systems data and Department of Veterans' Affairs client data. It will provide near real-time, actionable insights through a feedback loop designed to improve health, wellness, and safety outcomes. In the longer term, it will provide a whole-of-life view which will deliver insights into future service and compensation needs, based on serving military members' activity and incidents; and the ability to examine relationships between service exposure and subsequent Department of Veterans' Affairs claims.

Data from across the Defence enterprise is required to support this solution, along with Department of Veterans' Affairs data. Delivering on this initiative is a high priority for the Australian Government, Defence, and the Department of Veterans' Affairs. The uplift and management of data and analytics required to deliver the Data Sharing and Analytics Solution, funded through the 2021-22 Budget, will be prioritised across the life of the *Defence Data Strategy*. This will ensure the initiative delivers real benefits for Australian Defence Force members and veterans within the agreed timeframes.

Australian Geospatial-Intelligence Organisation's data journey

In 2018, the Australian Geospatial-Intelligence Organisation identified critical shortfalls in its governance and enterprise management of geospatial data, information and intelligence or GEOINT. Following a data governance review the GEOINT Data Office was established. Applying industry and government best practice models and principles we made positive changes to our enterprise data management practices. The Review also led to the development of the Foundation Geospatial Requirements Explorer tool and implementation of streamlined technical solutions to improve the management and flow of unclassified GEOINT data.

Together these changes ensure that:

- GEOINT data is treated and managed as a strategic national resource;
- GEOINT data requirements are captured; and
- Fit-for-purpose data is available in the timeframes needed to support critical Defence and national operations.

Prior to the release of the Foundation Geospatial Requirements Explorer tool in October 2020, we were receiving requests for foundation GEOINT data from Defence customers without the attribution required to conduct effective production planning, prioritisation, and de-confliction with our Allies.



Working in close partnership with Intelligence Capability Division, we built the tool to capture informed Defence strategic requirements. This allowed the Defence user community to request data, products, and services for operations, contingencies, and capabilities. Foundation GEOINT data production efforts can now be de-conflicted with current global data holdings and the results used to identify Defence's readiness in any given area or region.

With a clear understanding of Defence GEOINT data requirements, we have also streamlined data flows and architectures to ensure timely and effective delivery to the end user.

Prior to 2020, we were forced to move large GEOINT datasets across multiple systems and security domains before they were accessible to customers. This was a cumbersome process and it often led to delays in customers accessing GEOINT data. It also occasionally reduced the effectiveness of the unique support that we provide.

To address this problem, we worked closely with capability delivery and industry partners to develop a streamlined data flow and management process for unclassified GEOINT data. Applying best-practice data architecture principles, we built a workflow that automated the registration and flow of GEOINT data. This resulted in several benefits, including: allowing data to be moved across systems with a unique identifier and consistent management practices in all domains, reducing manual handling and expediting timeframes for data delivery, and GEOINT data dissemination from unclassified systems.

Our ability to deliver more value is a direct result of managing data well. The Australian Geospatial-Intelligence Organisation's first Data Strategy, AGO Data Strategy 2021-2025, will be released in the second half of 2021.

*GEOINT Data Office, Australian
Geospatial-Intelligence Organisation*



Australian Geospatial-Intelligence Organisation Remote Ground Station in Woomera. Photo Credit: Jarrod Lloyd.

MEASURING SUCCESS



How will we know we are making progress?



Across the five pillars there are 27 initiatives designed to build our data maturity and deliver real outcomes for Defence. The data uplift delivered through these initiatives will:

- Improve the agility and speed of our decision-making;
- Reduce the time and effort required to build an evidence-base;
- Help us better understand and manage capacity pressures and resource prioritisation;
- Strengthen our management of capability data requirements; and
- Deliver increased intelligence, situation awareness, and tactical advantage.

This is not a set and forget Strategy. The stakes are just too high.

This inaugural *Defence Data Strategy* focuses on implementing foundational initiatives to lift Defence's data maturity quickly over a two year period. It will be supported by a detailed implementation plan that will be delivered in Quarter 4 2021, after the establishment of the Chief Data Integration Officer and their initial review period.

Over this time, Defence recognises that we may need to adjust our approach and evolve with the environment, such as a changing technological landscape and the impact this has on data management practices.

Defence must ensure that we are making progress towards our vision that Defence's data is a strategic asset – we value it, protect it, and leverage it to deliver strategic and operational advantage. Given the two year timeframe we will need to know quickly what is working and what is not. The detailed implementation plan will include metrics for each initiative that evaluate the tangible benefits delivered to Defence.

Defence will build on our current data maturity baseline through annual assessments that determine progress from the perspective of our senior leaders, technical experts, and the whole of our workforce.

Evaluating progress over the next two years will also set the context and approach for the next Defence Data Strategy in 2023.

Implementation Roadmap

2021					2022				
July - December					January - June				
1.1 Appoint Chief Data Integration Officer and implementation team									
			1.2 Establish supporting functions under the Chief Data Integration Officer for data governance, assurance, security, policy, standards, professionalisation, literacy, analytics and visualisation, and innovation						
1.3 Develop a detailed implementation plan									
1.4 Develop the Defence Data Operating Model									
1.5 Establish the Defence Data Management Board									
1.6 The Chief Data Integration Officer will lead Defence engagement with Five Eyes and whole-of-Australian government data and analytics forums									
1.7 Incorporate Data into the Command and Management Fundamental Input to Capability									
			2.1 Establish enterprise-wide data and metadata quality standards and guidelines for different datasets						
			2.4 Deliver a Data Security Policy						
			2.5 Establish policy and standards for data storage and disposal						
						3.1 Establish and maintain an enterprise-wide data catalogue			
			3.2 Review the search functionality of Defence's information systems and intranet						
			3.4 Improve Defence's record management practises						
						3.5 Develop a library of simple clear, and easily accessible fact sheets and guides on record management			
						4.1 Build and implement mandatory foundational data literacy training			
						4.2 Develop a data training continuum			
4.3 Explore the feasibility of developing data specialist career streams for the Australian Defence Force									
4.4 Establish data job families for data analysts, data scientists and data engineers									
			4.5 Develop opportunities for exchanges and secondments						
				4.6 Make visualisation and business intelligence tools available to all Defence personnel					
			4.7 Provide training to Defence personnel						
5.1 Undertake a stocktake of data capabilities and tools to scale to an enterprise-level									
5.2 Establish new data custodians									
						5.3 Deliver an ethical use of data policy			
Workforce									
Capability Delivery									
Wellbeing of ADF members and their families									

Legend



Govern



Trust



Discover

Strategic Taskforces

Use

Share

Priority Data Areas



