Defence White Paper 2015
Public Submission

Enterprise Information Sharing and Management
as a Defence Capability

Prepared for: Department of Defence
Date: 27/10/2014
Table of Contents

ABOUT ARCHTIS 1
EXECUTIVE SUMMARY: INFORMATION SHARING AS A DEFENCE CAPABILITY 2
1. DEFENCE’S COMMITMENT TO INFORMATION SUPERIORITY 5
2. DEFENCE’S INFORMATION SHARING CHALLENGES 6
3. INFORMATION SHARING IS A TRUST PROBLEM. 6
4. INFORMATION SHARING REQUIRES CULTURAL CHANGE. 7
5. THE REQUIREMENT FOR AN ENTERPRISE INFORMATION SHARING ARCHITECTURE 9
6. LIVING STANDARDS AND OPERATIONAL VIEWPOINTS – NOT A PAPERWEIGHT 10
7. CONCLUDING REMARKS 10

About archTIS

archTIS, formerly known as BSTTech Consulting, has been working for many years in various capacities within Defence. Most recently the company spent two and a half years developing the Single Information Environment (SIE) Security Architecture (SIESA) for the Chief Information Officer Group. The value of SIESA to Defence was recognised earlier this year when it won the Defence Security Excellence Award. SIESA and other Defence projects have given archTIS visibility into the state of information management within Defence.

We are pleased to put forward our public submission as part of the Defence White Paper 2015 consultation process.
Executive Summary: Information Sharing as a Defence Capability

Information Superiority underpins the breadth of strategic, operational and tactical objectives discussed in the 2015 Defence White Paper Issues Paper. Secure information sharing, integration and interoperability are critical for delivering a decision-making advantage to our fighting force and to enable and strengthen cooperation with our allies and partners. As the Australian Defence Force has limited resources, it must ‘fight smarter’ to obtain and maintain the advantage over its potential adversaries. To fight effectively, Defence needs to excel in how it uses information.

From an industry perspective, Information Superiority appears to be a statement of intent rather than an actuality. While Information Superiority has been championed over the years under different names, mostly recently ‘Network Centric Warfare’ or NCW, these initiatives have not yet succeeded in achieving the sophisticated information capabilities implicit in the current Defence Capability Plan. Siloed systems and information assets still limit Defence’s ability to share high-value information between platforms, and across business functions, thus diminishing its ability to deliver the expected information-driven outcomes. The operational and financial costs of NOT having the required information sharing capabilities in place are and will be significant.

This is of grave concern given the numerous new capabilities currently being deployed or under development such as Joint Strike Fighter, Landing Helicopter Dock, Air Warfare Destroyer, Airborne Early Warning and Control, Unmanned Aerial Vehicles, and Army Battlefield Management, all of which require a sophisticated information sharing, integration, interoperability and management capability. This capability does not currently exist nor has it been adequately prioritised by Defence.

**Recommendation 1: That Defence establish Information Sharing and Management as a Defence Capability in its own right**

Everyone within Defence has a stake in its information, its security, its management and its appropriate sharing. Establishing a trusted Information Sharing and Management Capability, therefore, is a whole-of-enterprise requirement that must be addressed holistically to achieve maximum effectiveness and efficiency. Given the criticality of information for the success of all Defence Groups and Capabilities, it is strongly recommended that Defence stand up an Information Sharing and Management Capability (ISMC) to coordinate its information management outcomes.

This capability set would assist both the personnel and the agencies in determining the extent to which the credibility and reliability of the information must be assured; how it needs to be located, used, and managed; and how it must be made available, accessible and shared so that it is useable by those who need the information, when and where they need it. An ISMC would enable Defence to: minimise the risk involved in implementing cultural change, stop technology-led solutions, deliver the highest value outcomes they need, and to achieve these results at an affordable price.
The ISMC would embed the ability to securely manage dynamic information relationships within Defence’s unique operational landscape. It would support Defence’s mobile and deployed systems and not only leverage information assets residing in the Defence information environment, but also manage their interoperability with the systems of Australia’s allies and partners.

The ISMC would require:

- An appropriate Authority with the power to manage this capability across the Department of Defence and the Australian Defence Force. Currently there is no clear authority with the power to coordinate and direct information management outcomes across Defence Groups and statutory authorities,
- An Enterprise Information Strategy – incorporating mission objectives, information management and information technology strategies for the whole of Defence
- A Governance structure for identifying and reinforcing the vision, principles, roles and responsibilities of all stakeholders within the ISMC
- Funding prioritisation for ongoing capability development under the Defence Capability Program (DCP), and
- CIO Sponsorship.

There also may be a case to establish Information Sharing and Management as the ninth element of Defence’s Fundamental Inputs to Capability (FICs), given that information ultimately links all of the other eight FICs together.

Establishing an Authority and Governance structure would also greatly assist in breaking down the cultural, policy and technical barriers to information sharing that are present in Defence. Other initiatives could include the implementation of a Trusted Information Sharing and Assurance Program. By establishing and certifying custodians to manage, not own, information, Defence could progress from a siloed approach to information management to an ethos of trusted information sharing.

A governance structure, however, will make little headway in its objectives without clearly defined paths of communication and reporting or a baseline that can be used to measure the progress and success of the capability. What questions should the Board ask of its direct reports and which metrics do they use to measure the progress of the IMSC? To drive coherence and improved communication and performance throughout the organisation, an enterprise information sharing architecture is therefore critical to the implementation, development and sustainability of the IMSC.

An enterprise information sharing architecture would capture the vision, principles, roles, responsibilities, contributions, reporting structure, workflows and performance metrics for all of the ISMC stakeholders. It supports a risk-managed approach to implementing the ISMC:

a) by identifying and targeting those information assets and services that support and/or deliver the highest value to the Defence mission and
b) managing and mitigating the risks associated with the secure sharing (and sharing failures) of information between Defence personnel and our allied partners.
The highest value, highest priority Defence outcomes should be the first to benefit from a trusted ISMC.

**Recommendation 2: That Defence develop an Information Sharing Architecture to design, prioritise and securely deliver the information services required for the Capability**

An ISMC would focus initially on delivering high-value information to the right people, at the right time, and in the right way. In order to trust its information, Defence requires assurance concerning the integrity, provenance, confidentiality and privacy of its high-value information, and of the identities, systems and workflows (processes) that make use of that information. Moreover, appropriate controls need to be in place that enable the assured interoperability of all of the networks, systems and processes that make use of those high-value information assets.

To achieve these objectives, the ISMC must be architected so that Defence's identities, workflows, systems and information assets work symbiotically to meet both the mission outcomes and the required level of information assurance. The Architecture would also enable Defence to target and prioritise expenditure decisions. Adherence to the Architecture would ensure that all procurements and independent projects of work can be integrated and assured within Defence's broader Single Information Environment (SIE).

**Recommendation 3: that Defence enforce the use of the Information Sharing Architecture to direct (a) the integration and interoperability requirements of all DCP projects and b) the allocation of investment and resources within this Capability to deliver better mission outcomes for Defence**

The ISMC would use the Information Sharing Architecture to inform, guide and coordinate the information elements pertinent to Defence’s technical regulation authorities. This approach would standardise and manage the interoperability and integration risks related to managing information exchanges across Defence.

The Information Sharing Architecture would establish information sharing and management standards that can be enforced by the technical regulation authorities. Enforcing the use of the architecture would therefore result in consistency across the mission-critical capability sets.

**Recommendation 4: That Defence leverage its Information Sharing and Management Capability and take a stronger leadership role in the development of international information sharing and interoperability standards**

Establishing an IMSC should also be a strategic goal for Defence. It would provide Defence with the opportunity to establish a stronger position of influence in representing Australia’s national interests in international secure information sharing forums. Positioning itself as a leader in this field would also enable Australia to take a more proactive role in the information sharing and interoperability standards that ultimately affect us.
1. Defence’s commitment to Information Superiority

In comparison with our allied partners, Australia maintains a small defence force on a constrained budget. Defence capability acquisition and development decisions are therefore necessarily made “on the basis of Defence imperative and considerations of cost and risk” (Defence 2014 Issues Paper, p24). Defence must commit to the development of capabilities that enable Australia’s finite military resources to fight smarter and more effectively than its potential adversaries. In responding to Defence’s question “What Defence capabilities do we need now and in the future?”, archTIS strongly recommends that Defence commit to, authorise, and prioritise the development of Information Sharing and Management (ISMC) as a key Defence Capability in its own right. An ISMC would enable faster, more informed decision-making, and the ability to respond more quickly to emerging threats and changing political landscapes.

The availability of accurate and timely information is fundamental to the effective prosecution of military action and, as a result, has been a centrepiece of previous Defence White Papers and the Future Joint Operating Concept (FJOC). In WP2009, a force structure review of Defence determined a number of capabilities that were required for the future force of Australian Defence. Information superiority was prioritised in WP2009 as a force capability “required to give our forces a winning edge in comprehensive situational awareness, rapid decision making, networked capabilities, and the precise application of force”. WP2013 demoted information to being an enabling force rather than a force in its own right. This approach led to a focus on large ICT infrastructure investments rather than achieving information superiority and a more informed decision-making capability. It did, however, continue to highlight how reliant Defence operations, capabilities and platforms are on quality information to meet current and future mission outcomes.

The right information delivered to the right place, at the right time and in the right form multiplies the effectiveness of Defence capabilities in the maritime, land, air and space environments. Delivered across its agencies and units, relevant and reliable information services can facilitate Defence’s ability to make superior decisions concerning the protection of Australia’s interests, the promotion of stability and cooperation in our region, and the commitment of resources in support of peacekeeping, humanitarian and disaster relief operations. Even though Defence has long recognised that secure information sharing and management is critical for gaining and retaining military advantage, Defence still does not appear to have achieved the information capability it urgently requires.

**What capabilities does Defence need now, and in the future?** Information is THE most critical element of Australia’s evolving military capability. The success of all Defence Groups and Capabilities is reliant on Defence’s ability to gather, manage and share its information in a secure and timely way. **An Information Sharing and Management Capability (IMSC) is required to coordinate the information management outcomes of these Groups and Capabilities**, particularly those outcomes that are of high-value in terms of meeting the
Defence mission. Defence must acknowledge, prioritise and actively commit to implementing, developing and sustaining such a Capability.

2. Defence’s Information Sharing Challenges
There are a number of fundamental challenges that Defence must overcome to implement a successful information capability.

2.1. Information Sharing is a trust problem.

Secure sharing implies and requires a level of trust. In a risk-averse environment such as Defence, establishing trust is hard to achieve. While digital information once flowed primarily within the perimeter of an organisation and information was only shared hand-to-hand between people who knew each other, today’s information is being shared at a greater speed, with people we do not know, and often with less thought as to the risks presented by these exchanges. To compound the fear of exposure, events such as Snowden and Wikileaks have shown that even vetted personnel cannot always be trusted with the organisation’s most prized information.

Security models must now be redesigned to reduce both costs and risks while enabling the sharing of information from within existing perimeter protected domains. Often these attempts result in higher costs and unnecessary complexity. Redesigning the security model is further complicated by the proliferation of data, the way we source services, and the mobile workforce. Smart phones, tablets and other mobile devices have spearheaded a cultural change in the way we work and consume information. While perimeter and network security models are still relevant, organisations now need to extend security controls to the information itself so the data can be both mobile and secure.

Fear of information exposure, arising from mistrust in people and in systems, constrains Defence’s preparedness to share potentially mission-critical information. Without trust, personnel hesitate to share for fear of the consequences, the value and power of information is diminished, and strategic and operational objectives cannot be achieved. Therefore to meet its mission, Defence must find a way to share information in an assured manner.

Despite the need to better manage and share information, organisations often only address individual ICT symptoms, typically at the network or presentation layers. The problem with this approach is that the real threat is either already inside or can gain broad-base access to information by breaching the perimeter. Placing stronger security controls around an organisation is not sufficient to address the threat of the trusted insider. Perimeter security controls are a reactive method of dealing with information security – one that often works counter to the needs of the mission. Instead of facilitating the exchange of information between people, systems and organisations, perimeter security controls can inhibit information sharing, reinforce the proliferation of information silos and even encourage people to circumvent security in order to ‘do their job’.
Defence must be able to deliver the right information services when and where the organisation needs them. To achieve this goal, Defence must first establish:

- what information it has,
- the value of that information,
- which information assets and services the business consumes to make decisions,
- what information it needs to share with others outside the organisation, and
- which information outsiders might consider worth targeting.

Identifying the information that is of most value to the Defence mission, and that needs to be protected, is not a trivial activity. It involves a significant number of information stakeholders from across the operational units, information management and security domains. All of these information stakeholders must develop a deep understanding of, not only their own roles and responsibilities, but also their interrelationships within and beyond the organisation. Who supports whom? What are they relying on each other to provide and when? Who do they report to and how are they being measured? Can they trust their people, systems and workflows to manage the information that drives the organisation?

2.2. Information sharing requires cultural change.

The structure of Defence makes achieving quality information sharing and management more complex. Defence encompasses many groups, organisations, agencies and units who are all dependent on quality information to achieve their missions. Despite the diversity of these groups, they all contribute to meeting the over-arching strategic objectives of the Department. The number and distance between these groups, however, inclines Defence towards the accumulation of disparate stockpiles of valuable information. Often these compartmented information assets are not shared between agencies and personnel for all of the four main reasons outlined in this submission. Keeping information in isolation decontextualizes and devalues that information by not making it available to those who need it to make decisions concerning our nation’s security.

Apart from the intent in the 2014 Defence Capability Development handbook to focus on improving information management alignment, there do not appear to be any clear and authoritative guidelines for governance bodies and technical authorities that describe or govern how an enterprise-wide ISMC should be implemented and sustained in practice. Authorities and committees are only effective if they are appropriately informed, and have the authority to effect change and implement decisions coherently throughout the enterprise. If these bodies are not given the framework for determining the Capability’s development, they are less likely to achieve information integration and interoperability and Defence will continue to battle with the current state of its information services at home and abroad.

Ideally an ISMC would be managed or coordinated as a Capability in itself, or as a Fundamental Input to Capability (FIC), and be appropriately recognised within the
Capability Development process. It would have the appropriate Authority and Governance structures to enable the coordination, monitoring, and management of the Capability. Funding would be prioritised for ongoing development of the Capability under the sponsorship of the CIO. Formally establishing the Authority and Governance for the ISMC would also greatly assist in breaking down the cultural barriers to information sharing that are present in Defence.

Other initiatives such as a Trusted Information Sharing and Assurance Program should also be rapidly deployed to develop an ethos of trusted information sharing within Defence. This certification program would encourage mutual recognition of authorities and information ‘consumers’ by establishing information holding responsibilities, levels of trust and assurance required, information sharing practices and identity/attribute management capabilities. In an environment where the desire to ‘own’ information assets is encouraged by the cultural and structural environment, this type of program could help remove this barrier. It would certify ‘information custodians’ to hold, not own, information, and help them to understand and confidently apply the terms and conditions of sharing information within Defence and with its partners.

2.3. Information Sharing is not a technical problem.

The technical capability to share information securely already exists. Enabling information sharing and management systematically across numerous groups, however, is a significant integration interoperability issue for Defence. Projects of work that are undertaken independently can often achieve great success in terms of localised outcomes, but do not contribute to the over-arching interoperability objectives of Defence as a whole. Without an enterprise framework and set of standards to use as guidance, these isolated projects will continue to proliferate – utilising funding and resources, and delivering outcomes that are incapable of delivering enterprise value to other Capabilities. The ISMC requires an enterprise information sharing architecture to design an information strategy and implementation plan for Defence; establishing the mechanism to inform policy and risk management strategies, improve procurement processes, make better resource and funding allocation decisions, and deliver the right information services in support of the Defence mission.

2.4. Information Sharing must be recognised as a business problem.

Mission objectives and organisational outcomes are difficult to achieve if the supporting information environment is not aligned to deliver the information and services required. Compartmented or siloed information that is not shared in a timely and appropriate way can result in serious consequences such as loss of life, threat to infrastructure, mission compromise and operational failure. Command and control decisions need to be made on the right information, and not based on faulty assumptions or corrupted data sets.

The mission and economic costs of NOT sharing information are significant. The costs of maintaining a siloed information environment are high, not only in terms of life and operational outcomes, but also in terms of:
• the resource costs involved in supporting duplicate information systems, networks, and data warehouses, and
• meeting existing and evolving regulatory, legislative, policy and security compliance requirements.

Information sharing touches all aspects of Defence operations. It is not just an ICT or information security problem to resolve. Striking the balance between protecting and sharing information requires a coordinated, integrated effort on behalf of Defence as a whole enterprise. All high-value information stakeholders need to work together under a coherent framework to:

• better understand the organisation’s high-value information requirements
• implement a trusted information sharing and management capability that both enables AND controls information availability and access, and
• develop a unifying framework for operational productivity, undertaking programs of work and responding to changing information needs.

By taking a whole-of-enterprise approach, these goals can be achieved by integrating Defence’s operational needs, good information management practices and dynamic security controls in a symbiotic way.

3. The Requirement for an Enterprise Information Sharing Architecture

Enterprise Architecture is a proven approach for capturing the agreed business outcomes of all stakeholders and translating them into defined information, governance, and technology requirements for the enterprise. Such an architectural approach should be used to systematically capture, analyse, design and implement the Defence Information Sharing and Management Capability. An Enterprise Information Sharing Architecture will capture and communicate stakeholder’s requirements at different functional levels of the organisation. The COO or CIO, for example, requires different information to make and communicate an investment decision than a system engineer who is developing and implementing an ICT system. To ensure that the needs and goals of stakeholders operating at all levels of the organisation are met, effectively communicated and aligned, an architectural approach is used to describe the enterprise information sharing requirements from different stakeholder viewpoints.

Enterprise Architecture is a systematic, proven and practical approach to aligning the strategic mission intent with the most effective means of meeting current and future objectives. It also provides a baseline for comparing and integrating architectures, protocols, systems and assets in a consistent way. As a result, an Enterprise Information Sharing Architecture is THE key success factor for implementing and governing the ISMC.

3.1 Benefits of an architectural approach

By guiding the development and implementation of agile information services and infrastructures, an Enterprise Information Sharing Architecture would determine how
Defence can focus its limited ICT resources and investments on the most critical information services. The architecture would:

- Identify which information services, and their supporting capabilities, drive decision-making superiority throughout the enterprise;
- Maximise efficiencies and reduce cost through the identification and targeting of high-value investments and their precise procurement requirements;
- Determine the appropriate balance between sharing and protecting information;
- Describe enterprise information services in terms of their business value (e.g. assurance, compliance, quality, timeliness, etc);
- Manage risks in relation to interoperability and integration;
- Establish, mature and expand the information services appropriate to Defence's unique context;
- Leverage existing information infrastructure and capabilities, and
- Maximise the use of COTS products according to need.

The Enterprise Information Sharing Architecture would necessarily leverage Defence’s recently endorsed Security Architecture for the SIE (SIESA), and embed these security controls throughout the broader enterprise information sharing and management capability.

4. Living Standards and Operational Viewpoints – Not a Paperweight

For the ISMC to become a reality, the architecture must be applied and enforced within the context of a governance structure. Solution design, training, implementation and support services should also be governed and directed by the architecture so that the ISMC can be sustained and continually improved to meet the dynamic and emerging needs of Australia’s Defence. An applied architectural approach is recommended by archTIS as the best means to address the interoperability and integration risks related to the management and sharing of information throughout Defence and with its allied partners.

At present, Australia’s allies dominate decisions regarding multinational information sharing. Undertaking the ISMC would provide Australia with the experience and expertise to further influence international interoperability and information sharing standards, protocols and policies, and better serve the interests of Australia.

5. Concluding Remarks

Defence urgently needs to implement a Defence Information Sharing and Management Capability and its associated guiding architecture. While the need for this capability has been outlined in previous White Papers, the intent has not been fully realised. archTIS hopes that this submission might encourage a clear commitment in Defence White Paper 15 regarding the intent, meaning and action required to realise this critical information capability set, and in doing so contribute a vital winning edge to Australia’s future fighting capabilities.