Introduction
This paper is written following the forum at the Australian Strategic Policy Institute with the Defence Whitepaper team. The paper was requested to be brief and so is necessarily short and only summarises the concepts provided. Recordkeeping Innovation would be interested in undertaking a more detailed analysis and report if required. Recordkeeping Innovation agrees to the publication of this document

Executive Summary - An overview of Information Governance - why is this important?
The Australian Defence Force relies on information that must be authentic, reliable, accessible and useable. ADF creates and receives information as a key part of conducting its activities, information that is valuable for re-use, to provide robust and accountable systems, and to provide trustworthy and reliable information. Information in all formats, but particularly digital information, must meet certain standards if it is to support evidence based decisions and actions that can be reviewed, audited and assessed. Sound information management is closely aligned with risk management and the ability of ADF to operate efficiently across multiple geographic locations. Standards for information governance are becoming more complex with the wide range of communication tools, formats and platforms.

This requires a systematic, standards based approach to both take best advantage of the technology opportunities, while also enabling information that is trustworthy, easily found (within security restrictions) and accessible.

What are the key characteristics of records?
The terms information and records are often used interchangeably. Defence receives information created by others and analyses this information to assess risks and determine what actions to take. The source and credibility of this information is essential to assess those risks, so the value of the information can be properly assessed. Information is an asset that requires a level of management.

Records are a sub-set of information, and describe the data that is created as evidence in the course of conducting activities. Records must be created, captured and managed into systems, organised and made available in accordance with Defence’s well established business rules and security settings. These are defined in the operational procedures, methods and command structures, describing what records must be created, what data should be included, who authorises actions etc. These business rules are represented in the information structures that determine who has permission to access, use or re-purpose records and information.

Key questions:
- What data is needed?
- Where is data collected and how is the process documented?
- Do we know what information we have?
- If we find data, can it be used, and is it in an accessible format?
- Where is the data stored?
- Who can access it?
- How long is it valid and for how long should we keep it?
- How can we find, interpret the data?
- Is it the right version?
- Once collected, can it be re-purposed?
Records support effective ADF activity; they are used to inform what was done and how to do business in the future.

The context (what business was being conducted to create records) is just as important as the content, so that records can be understood and interpreted by others. Metadata provides this essential context, and metadata is critical for managing digital data.

Records are created to meet accountability, public expectations and to satisfy legislative responsibilities – who may act, decide, inform.

What’s the current framework for digital information?
Defence has previously established sound infrastructure for managing paper records (registries) with control systems to manage creation (forms, delegated authority); capture and registration; naming and tracking. These controls have been partially transferred into digital records, but the digital environment is challenging, not least because of the proliferation of formats, multiple repositories, duplication and the ease of creating. The volume of digital data is growing exponentially and is difficult to control.

![Diagram illustrating the problem with digital formats and multiple storage repositories.](www.archives.govt.nz)

There are international and local standards that can help to reduce the complexity of managing digital information.

Why is information important?
Like all government agencies, ADF needs to rely on evidence based decisions, drawn from accurate information, that is delivered in a timely manner. Information must be accessible when it is needed. When delivered, it must be authoritative and accurate.

A key question in deciding ADF capabilities is “What Science and Technology capabilities are critical to underpin our broader defence capabilities?” To support ADF capability, reliable information is vital.

Technology is an important delivery mechanism for rapid information access, however technology alone will not deliver the outcomes need by ADF to support current and future operations.
In the absence of the proper information governance framework (roles, rules, policies and practices), having these holistically applied and understood, the ADF may be relying on information that is potentially misleading.

What does Information Governance involve?
Information governance is the set of roles, assigned responsibility, policies, procedures, processes and practices and controls to manage information. These are needed at an enterprise level to support ADF’s current and future regulatory, legal, risk, environmental and operational requirements.

Information Governance delivers the basis for:

- ensuring that the source, links, date and reliability rating of the information are known (authenticity and reliability);
- that the information’s context, format and security is understood and documented (accessible and useable) through metadata;
- privacy / security attributes are known and implemented;
- search and find requirements are defined and applied;
- storage is optimized based on currency; and
- access/retention is monitored.

Appropriate structures for information will aid better searching and retrieval, reduce the time wasted on searching and reviewing information and improve relevancy, currency, and ensure that information is valid.

What are the benefits?
These benefits were achieved by government agencies that now operate in a fully digital environment in a recent survey reported by National Archives.

For instance, if 20% of the ADF Uniform and Civilian staff spend 10% of their time searching for information, that costs the ADF $73 million. If that time can be reduced by 30% this represents a saving of $22 million.

---