Foreword
by Senator the Hon. John Faulkner
Minister for Defence

Defence's strategic objectives and the information and communications capabilities needed to achieve them are inextricably linked.

The size and complexity of the Australian Defence Organisation presents a number of governance issues for strategic planners.

Defence is one of the largest telecommunication providers in the country. Information and communications technology (ICT) related planning in Defence has to allow for the communication needs of military personnel in the field, the secure transfer of information between the Australian Government and its allies and the architectural challenges faced when connecting people, planes, ships and land vehicles to a single information environment - all in addition to the standard ICT requirements of over ninety thousand corporate users.

Defence ICT planning has to meet an extremely diverse list of needs. This strategy has been written with those challenges in mind.

There will be a whole-of-portfolio approach to considering ICT investments and planning, increasing efficiency and streamlining processes. The areas, agencies and branches directly affected by new ICT projects will play a direct role in determining project priorities and timing. Put simply, investment decisions will reflect departmental priorities, and end users will help shape the specifics of what they get, and when they get it.

Cultural change and workforce planning initiatives will make the most of our ICT workforce, and the new Integrated Defence Architecture will guide future investment decisions and the strategic planning of information technology and systems.

This ICT strategy also places the remediation and reform of ICT capability provision within the broader context of the 2009 Defence White Paper and Defence's Strategic Reform Program (SRP).

In the years ahead, our information and communications capabilities will be more important than ever before in making sure our men and women in uniform, and the many thousands of people who support them, have all the tools they need to carry out the tasks the community needs and expects from them.

This document sets out the steps we are taking to make sure our ICT is up to the challenge.

Senator the Hon. John Faulkner
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>1</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>5</td>
</tr>
<tr>
<td>Objectives</td>
<td>5</td>
</tr>
<tr>
<td>Introduction</td>
<td>7</td>
</tr>
<tr>
<td>Governance and the Role of the CIO</td>
<td>7</td>
</tr>
<tr>
<td>Savings</td>
<td>8</td>
</tr>
<tr>
<td>Success</td>
<td>8</td>
</tr>
<tr>
<td>Strategic Interests and Defence Priorities</td>
<td>11</td>
</tr>
<tr>
<td>Information and Communications Technologies to 2030</td>
<td>12</td>
</tr>
<tr>
<td>ICT Impact on Operations</td>
<td>13</td>
</tr>
<tr>
<td>Interoperability Trends</td>
<td>14</td>
</tr>
<tr>
<td>Commercial and Regulatory Trends</td>
<td>15</td>
</tr>
<tr>
<td>Strategic Imperative One: Optimise Value of Defence ICT Investment</td>
<td>17</td>
</tr>
<tr>
<td>Improve ICT Cost Transparency and Stakeholder Communication</td>
<td>17</td>
</tr>
<tr>
<td>Prioritise for Effective ICT Spend</td>
<td>19</td>
</tr>
<tr>
<td>Optimise Project and Operations Efficiency</td>
<td>20</td>
</tr>
<tr>
<td>Harmonise with Whole-of-government Initiatives</td>
<td>20</td>
</tr>
<tr>
<td>Key Benefits</td>
<td>21</td>
</tr>
<tr>
<td>Strategic Imperative Two: Closer Stakeholder Engagement and Alignment</td>
<td>23</td>
</tr>
<tr>
<td>Improve Alignment Between Stakeholder Needs and ICT Capabilities</td>
<td>23</td>
</tr>
<tr>
<td>Portfolio Management Office</td>
<td>25</td>
</tr>
<tr>
<td>Aligning ICT Organisation with Stakeholders</td>
<td>26</td>
</tr>
<tr>
<td>Organisational Model Explained</td>
<td>27</td>
</tr>
<tr>
<td>Become Easier to Work With</td>
<td>27</td>
</tr>
<tr>
<td>Design Solutions Collaboratively with Stakeholders</td>
<td>28</td>
</tr>
<tr>
<td>Implement Defence-wide ICT Governance</td>
<td>28</td>
</tr>
<tr>
<td>Key Benefits</td>
<td>29</td>
</tr>
<tr>
<td>Strategic Imperative Three: Provide Agreed, Priority Solutions</td>
<td>31</td>
</tr>
<tr>
<td>Stabilise and Secure ICT</td>
<td>31</td>
</tr>
<tr>
<td>Consolidate, Standardise and Optimise ICT</td>
<td>32</td>
</tr>
<tr>
<td>Addressing New ICT Requirements</td>
<td>32</td>
</tr>
<tr>
<td>Leverage Emerging Technologies to Address New Business Needs</td>
<td>33</td>
</tr>
<tr>
<td>Create and Adopt an Enterprise Architecture</td>
<td>33</td>
</tr>
<tr>
<td>Enterprise Solutions</td>
<td>35</td>
</tr>
<tr>
<td>Key Benefits</td>
<td>36</td>
</tr>
</tbody>
</table>
Strategic Imperative Four: Strengthen ICT Capability 37
   Energise the Culture 37
   Strengthen ICT Leadership 38
   Improve Processes and Tools 39
   Moving to a Shared-Services Model 39
   Professionalise the Workforce 39
   Workforce Planning 40
   Leverage Vendors and Sourcing 41
   Effective Resource Planning and Management 42
   Key Benefits 43

Outcomes and Benefits of this Strategy 45
   Greater ICT Scalability, Flexibility and Adaptability 45
   Improved Information Speed and Accuracy 45
   Continued Technological Capability Edge 45
   Enhanced Interoperability 46
   Improved Business Support 46

Implementing our ICT Strategy 47
   ICT Reform Program 47
   ICT Work Plan 48

   Implementing Strategic Imperative One: Optimise Defence ICT Investment 49
   Initiative: Consolidate Data Centres 49
   Initiative: Reduce ‘Time to Market’ ICT Two Pass Process 49
   Initiative: Implement a Single Secure Desktop 49
   Initiative: Develop Defence’s Enterprise Architecting Capabilities 50
   Initiative: Implementing a Services Oriented Architecture 50
   Initiative: DIE Simulation and Modelling 50
   Initiative: Centralised Services - Deliver Distributed Computing 50

   Implementing Strategic Imperative Two: Closer Stakeholder Engagement & Alignment 51
   Initiative: New Stakeholder Engagement Model 51
   Initiative: Improved Sharing and Access to Services with Key Allies 51
   Initiative: Specialist Business Solutions Design Capability 51

   Implementing Strategic Imperative Three: Provide Agreed, Priority Solutions 51
   Initiative: Information Management 51
   Initiative: Deliver Unified Communications 52
   Initiative: High Speed Strategic Communications Network (JP 2047) 52
   Initiative: Analysis of Disruptive Technology 52

   Implementing Strategic Imperative Four: Strengthen ICT Capability 52
   Initiative: Sourcing Strategy 52
   Initiative: Investing in People 53
   Initiative: IT Service Management 53
   Initiative: ICT Reform Portfolio Management 53
   Initiative: CIO as Coordinating Capability Manager 54
   Initiative: Infrastructure Remediation 54

Enabling Defence Business Reform 54

Glossary, Abbreviations and Acronyms 57
Executive Summary

In the current environment, Defence's information and communications technology (ICT) systems are being challenged more than ever. Australia's Defence personnel expect to see capability improvements resulting from integrated and network-enabled platforms, administrators expect ICT enhancements to provide business process efficiencies and the ICT threat environment is becoming more hostile.

The ICT strategy has been developed to address shortcomings in governance, planning and control frameworks for ICT. Defence is also establishing clear lines of accountability and transparent management responsibilities at the most senior levels, as well as investing in critically under-funded capabilities to improve its ICT infrastructure.

Objectives

After wide-spread engagement and consultation across Defence five clear objectives regarding Defence's future ICT environment were identified. These are:

- greater ICT scalability, flexibility and adaptability
- improved information speed and accuracy
- continued technological capability edge
- enhanced interoperability
- improved business support

Achieving those objectives will require strategic reforms, as outlined in the Defence Strategic Reform Program, as well as reform of ICT processes, systems and workforce arrangements. These reforms will enhance Defence's ability to develop ICT capabilities by allowing stakeholders to prioritise their ICT funding, and will optimise the structure of Defence's ICT workforce to deliver reliable, high-quality solutions.

To achieve these objectives this strategy is based on four strategic imperatives:

1. Optimise the value of Defence's ICT investment through cost transparency, improved stakeholder communication, prioritisation of spend and efficiency in ICT activities.
2. Drive closer alignment with stakeholders through a stakeholder-centric organisation model, improving engagement and driving towards a collaborative approach to developing ICT capabilities.
3. Provide agreed, priority solutions through the establishment of a Defence-wide ICT Operating Model and Enterprise Architecture promoting standardisation and consolidation.
4. Strengthen ICT capabilities through improvements to culture, leadership, processes, skills, sourcing and resource planning.
Figure One: Defence ICT Strategy

Mission: Lead the integrated design, cost effective delivery and sustained operation of the Defence Information Environment.

<table>
<thead>
<tr>
<th>1 Optimise Value of Defence ICT Investment</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Improve alignment between stakeholder needs and ICT capabilities</td>
</tr>
<tr>
<td>b. Aligning ICT organisation with stakeholders</td>
</tr>
<tr>
<td>c. Become easier to work with</td>
</tr>
<tr>
<td>d. Design solutions collaboratively with stakeholders</td>
</tr>
<tr>
<td>e. Implement Defence-wide ICT governance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2 Closer Stakeholder Engagement &amp; Alignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Improve ICT cost transparency &amp; stakeholder communication</td>
</tr>
<tr>
<td>b. Prioritise for effective ICT spend</td>
</tr>
<tr>
<td>c. Stabilise &amp; secure ICT</td>
</tr>
<tr>
<td>d. Aligning ICT organisation with stakeholders</td>
</tr>
<tr>
<td>e. Create &amp; adopt an enterprise architecture for ICT in Defence</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3 Provide Agreed, Priority Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Stabilise &amp; secure ICT</td>
</tr>
<tr>
<td>b. Consolidate, standardise &amp; optimise ICT</td>
</tr>
<tr>
<td>c. Addressing new ICT requirements</td>
</tr>
<tr>
<td>d. Leverage emerging technologies to address new business needs</td>
</tr>
<tr>
<td>e. Create &amp; adopt an enterprise architecture for ICT in Defence</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4 Strengthen ICT Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Energise the culture</td>
</tr>
<tr>
<td>b. Strengthen ICT leadership</td>
</tr>
<tr>
<td>c. Improve processes &amp; tools</td>
</tr>
<tr>
<td>d. Professionalise the workforce</td>
</tr>
<tr>
<td>e. Leverage vendors &amp; sourcing</td>
</tr>
<tr>
<td>f. Effective resource planning &amp; management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Intelligence &amp; Security Services</th>
<th>Military Capability</th>
<th>Corporate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interoperability</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Introduction

Over recent years there have been a number of reviews relevant to the operation of ICT services within Defence.

In 2006 the government announced a review of the organisational efficiency and effectiveness of Defence, including its information management processes and systems. The resulting report was issued in 2007 as the Defence Management Review (DMR). Several recommendations were made in relation to ICT, including the proposal that Defence develop an enterprise-wide ICT strategy. In its response Defence agreed, recognising the need to link ICT investment decisions to business priorities with robust, transparent processes.

While developing this strategy Defence also commenced work on a new White Paper and elements of this ICT Strategy were incorporated into the White Paper’s ICT Companion Review.

At the whole-of-government level, the Department of Finance and Deregulation commissioned Sir Peter Gershon to undertake an independent review of government’s use of ICT. Although Defence was not officially a subject of the Gershon Review, the Secretary of Defence maintained contact with Sir Peter Gershon throughout the strategy development process.

Governance and the Role of the CIO

The key elements of the Defence ICT Strategy are described in the body of this document, particularly in the strategic imperatives. It is useful however, to begin with an explanation of the role of the Chief Information Officer (CIO) in the provision, sustainment and governance of Defence ICT.

In 2008 the Secretary and Chief of Defence Force (CDF) established the Defence ICT Committee (DICTC) to provide a strategic focus on investment in Defence ICT Capability; and in 2009 the DICTC confirmed the appointment of the CIO as the Coordinating Capability Manager of the Defence Information Environment (DIE). In announcing the appointment, the DICTC confirmed the CIO’s responsibility for ongoing development of the DIE, controlling sustainment costs, and enabling Defence to take advantage of emerging technologies.

Furthermore the DICTC confirmed that the Defence CIO is now responsible and accountable to the Secretary and CDF for:

- The development of Defence ICT policy, concepts and doctrine
- Advising all Defence Committees on ICT issues
- Developing a single Defence ICT architecture, including standards and product lists
- Establishing priorities and engagement strategies for ICT interoperability with other Australian Government agencies, allies and coalition partners
- Coordination of ICT related fundamental input to capability issues
- Establishing the governance mechanisms necessary to allow the execution of these responsibilities and accountabilities
To support the CIO in this role, the DICTC will continue to consider, review and prioritise all ICT initiatives and expenditure across Defence.

All ICT funding decisions will be made within the context of a single Defence-wide ICT portfolio, reflected by a unified Defence ICT Work Plan and implemented by the Defence-wide ICT workforce. This will in turn enable decisions and trade-offs to determine which ICT projects Defence can afford and allow the Chief Information Officer to execute his role as the Coordinating Capability Manager for Defence ICT.

New governance arrangements will align ICT investments across Defence with the priorities set by the Secretary and Chief of the Defence Force. New procurement and approval processes for ICT investments will shorten time to market while maintaining high levels of project assurance.

...governance arrangements will confirm that all ICT investments across Defence are aligned with the priorities set by the Secretary and Chief of the Defence Force.

The implementation of a single portfolio of ICT investment in Defence will increase the visibility of Defence’s ICT expenditure and improve the effectiveness of Defence ICT systems and processes.

**Savings**

Remediation and reform in the form of a consolidated, standardised Defence Information Environment (DIE) will deliver savings and performance improvements. By 2012 the ICT reform program will build an improved DIE to support Defence war fighting and business reform objectives through to 2030.

...deliver savings and performance improvements through a consolidated, standardised Defence ICT environment.

This reform will require an investment of around $940 million over the next four years but is expected to deliver savings of $1.9 billion over the decade and around $250 million per annum thereafter.

**Success**

Successful implementation of the Defence ICT Strategy will lead to several key outcomes.

The DIE will be one network connecting fixed and deployed locations built on a single set of standards and products. It will encompass all security levels and will determine that the right person has the right authority to access information.

A typical desktop set up available to all Defence sites will be a single screen connected to a network that can display multiple security sessions. Secure voice and video will be available to the desktop in most fixed and deployed locations. Wireless networks will also be considered in appropriate locations.
Deployed commanders and decision makers will have a single view of the battle space through a Common Operating Picture accessing a wide range of data from sensors and sources.

Finance, payroll and personnel information will be easily accessed, manipulated and aggregated by authorised Defence staff. New capabilities such as the automation of procurement, personnel and pay administration, vetting, recruitment, estate management and performance reporting will be progressively introduced.
Strategic Interests and Defence Priorities

The 2009 Defence White Paper has affirmed the government’s commitment to the Defence of Australia, the protection of our sovereign interests and the security and stability of our region. The document also articulates the strategic priorities for all areas of Defence and lays out the government’s future plans for the development of Force 2030.

Australia’s most basic strategic interest remains the Defence of Australia against direct armed attack... founded on the principle of self-reliance in the direct Defence of Australia.

As one of the key force attributes that guide the development of Force 2030, the 2009 Defence White Paper identifies ‘networked capability’ as helping our people to work more effectively together, providing common battle space awareness and, most crucially, helping to ensure information superiority over an adversary. This will allow our people to make critical decisions on the battlefield faster and with better knowledge than the adversary.

...the principal task for the ADF is to deter and defeat armed attacks on Australia by conducting independent military operations.

Defence will build a networked ADF. Modern technology will be used to link sensors, weapons systems, commanders and their personnel in a networked environment. The networked force is to be built by progressively delivering networked capability within the maritime, land, aerospace and intelligence, surveillance and reconnaissance (ISR) domains. This approach to building a networked Australian Defence Force (ADF) will be dependent on the establishment of a secure high-capacity information network that allows personnel located in different areas to collaborate in real-time and to precisely synchronise their operational actions.

The 2009 Defence White Paper gives priority to enhancing key areas of joint ADF capability.

Another crucial characteristic of our future ADF identified in the 2009 Defence White Paper is the adoption of a joint approach that binds single-Service capabilities and systems into an operationally seamless whole. Joint operations involving the three Services, other Defence agencies and, in some cases, other government agencies are to be the standard mode of operating for the ADF.

Australia must have the capacity to employ military power in collaboration with our allies and coalition partners, and must be willing to lead military coalitions when necessary to secure relevant shared strategic interests. In other cases Australia must contribute to military coalitions when it is in Australia’s clear interest.
to do so. To that end it is important for the ADF to develop and maintain a network of Defence partnerships as an important foundation for being able to work together when required. This will require increased interoperability between the ADF and selected allies and coalition partners, such as the United States, New Zealand and our partners in the Five Power Defence Arrangements, which includes the United Kingdom, Singapore and Malaysia.

As Defence reforms its ICT capability provision it will first need to remedy the fragility and other shortcomings of the current ICT environment. There is an urgent need to address long-term underinvestment in ICT infrastructure that has resulted in a significant proportion of Defence assets being beyond their effective life. Secondly, Defence needs to reform the way we use ICT to conduct our core and non-core business. Defence needs to continuously re-examine the manner in which ICT can assist our people and enhance processes and tools.

Thirdly, ICT reform is integral to the delivery of administrative savings across Defence. Better ICT management will result in savings to the portfolio as we standardise, rationalise, consolidate and re-use. Finally, business reform across Defence depends upon the effective implementation of ICT reform.

Optimising Defence’s ICT environment will be essential to delivering Force 2030. This includes our systems and processes, architecture and the skills of our workforce. Fixing problems and introducing new ICT capabilities that are aligned to Defence priorities will be the focus. At the release of the 2009 Defence White Paper, the government announced that it would invest more than $940 million over the next four years to reform and remediate the DIE and its supporting infrastructure. Two thirds of that will be used to address long-term underinvestment in Defence ICT by reforming access to, and management of, Defence information. The remainder will be spent on replacing obsolete hardware and improving information security.

The reform program will deliver business efficiencies and lower long-term costs. These initiatives are consistent with the recommendations in the Gershon Review into the Australian Government’s use of ICT and the outcomes sought from that review.

The reform program will deliver business efficiencies and lower long-term costs.

Information and Communications Technologies to 2030

Cognisant of the rapidly changing ICT environment and its on-going impact on Defence, a number of reviews drawing upon broad Defence representation sought to identify the scope of ICT issues to be addressed to 2030. The findings of these reviews helped to shape this ICT strategy.

Defence ICT capability needs to provide global communications and systems to support decision-makers at the tactical, operational and strategic level. Defence ICT capability is required to support headquarters staff, operational assets, intelligence surveillance and reconnaissance, targeting and navigation needs, logistics, medical and personnel systems.
Defence ICT capability needs to provide global communications and systems that support decision-makers at the tactical, operational and strategic level.

ICT Impact on Operations

The ongoing development of new ICT capabilities is creating both opportunities and challenges for the Australian Defence Force. On the one hand, improvements to Defence ICT will enable enhanced ADF decision-making and operational effectiveness. On the other hand, the use of emerging and relatively inexpensive ICT capabilities will also be available to adversaries. The ADF must continue to develop, deploy and exploit advanced ICT to operate successfully in this future battle space.

Control of the future battle space will be dependent upon the capability of Australia to develop, deploy and exploit advanced information and communications technologies.

Defence will leverage ICT capabilities to plan for and implement the full spectrum of tasks assigned to it by government, connecting whole-of-nation capabilities in an environment of increased uncertainty and reduced warning times.

This will require a holistic approach to ICT capability, integrating both war fighting and business functions so that technology enables the information access and functionality needed to accomplish the mission. To support this, Defence will create a single information environment with an efficient standard for ICT support to all functions. By developing a single information environment Defence will be able to better meet the demands of the strategic user as well as deployed and mobile users.

Through... a single information environment Defence will be able to support the strategic user as well as the deployed and mobile user.

Improved information management and sharing will enhance joint, multi-agency and coalition interoperability. This will reduce the disadvantages caused by regional factors and mitigate the risks associated with asymmetric threats.

The ability to lead and act decisively in Australia's primary area of strategic interest will involve developing robust ICT capability through investment in critical infrastructure such as satellite communications, and sufficient spectrum and network bandwidth to meet demand.

...to lead and act decisively in Australia's primary area of strategic interest will involve developing robust sovereign ICT capability.
ICT solutions need to comply with the technical standards of the weapon systems they may integrate with. Defence will develop a system for design-approval and consideration of the implications for ‘battle worthiness’. Defence will also need to revise its battle space architecture. Acquisition strategies should include consideration of Fundamental Inputs to Capability, and sustainment and recognition of lifecycle management requirements.

More agile procurement and adaptation cycles are required to prevent obsolescence and to maintain interoperability. Governance arrangements and Defence business processes will need to be subject to on-going review. Business processes must accommodate evolving military and commercial technology. Inefficient processes cannot be allowed to impact upon the delivery of new capabilities. ICT procurement risks and the Defence Capability Plan will be better balanced against the risk of obsolescence to maintain Defence’s technological competitiveness in Australia’s region.

Interoperability Trends

The ability to operate with other agencies both domestically and internationally is a key Defence capability enabler. Whether Defence is acting cooperatively with another Australian Government agency or operating as part of an international coalition, the ability to exchange data quickly and confidently is essential. Defence will develop a coordinated and robust exchange architecture to underpin these interactions.
The ability to interoperate with other agencies, both domestically and internationally; is a key Defence capability enabler.

Defence requires mandated architecture policies and an effective governance framework to enable interoperability. The Defence enterprise architecture must accommodate both government and Defence interoperability priorities in support of Defence’s requirements to interact domestically and internationally.

Commercial and Regulatory Trends

Defence ICT investment needs to deliver measurable value to Defence operations and business. Defence will continuously develop its ability to measure, benchmark and explain the business value delivered through investment in ICT.

Defence ICT investment will need to demonstrate the delivery of measurable value to Defence business and operations.

Defence will consider the implications of globalised information service providers beyond prime contracts. Defence has evolved over the past decades to become dependent upon a wide range of commercial services for its core business. These strategic service providers are transitioning into a globalised market driven by global economic forces and Defence needs to manage potential third party relationships. Defence will increasingly need to manage the risk and cost aspects of its commercial relationships and contracts.
Strategic Imperative One: Optimise Value of Defence ICT Investment

This first strategic imperative will maximise Defence's return on ICT investment by ensuring effort and expenditure is aligned to Defence's business needs.

Strategic Imperative One can be broken down into four strategic elements:

- Improve ICT cost transparency and stakeholder communication
- Prioritise for effective ICT spend
- Optimise project operations and efficiency
- Harmonise with whole-of-government initiatives

Successful delivery of those elements will enable Defence to clearly identify ICT accountabilities and responsibilities, improve cost transparency and stakeholder communication, establish governance mechanisms for resource allocation and improve the efficiency of ICT services and support.

Improve ICT Cost Transparency and Stakeholder Communication

Defence will adopt a portfolio management approach to its ICT investment, dividing business needs into Intelligence, Military, Corporate and Infrastructure categories.

An enterprise-wide Defence ICT Work Plan (The Work Plan) will align all ICT expenditure with the priorities set by government, the Secretary and the Chief of the Defence Force.

The Secretary and Chief of the Defence Force have appointed the Chief Information Officer (CIO) as the Coordinating Capability Manager for the whole of the Defence Information Environment (DIE). CIO will support the newly established Defence ICT Committee (DICTC), chaired by the Secretary and Chief of the Defence Force, and comprised of senior Defence leaders.

This high-level committee has overall responsibility for ensuring that the Defence portfolio's ICT expenditure is aligned to Defence priorities. It will aim to enhance the development of the Defence information environment, to control sustainment costs and to take advantage of emerging ICT technologies.
Figure Two below shows the structure of the Sub-Portfolio Committees, with definitions captured in Table One. Based on the current strategic needs of Defence, investment will be prioritised through the DICTC. It is expected that the definitions will undergo further refinement with stakeholders. This will be aligned to the Defence SRP, Defence Planning, and Defence Business Model.

Figure Two: Defence ICT Sub-Portfolio Committees
Table One: Definition of the Four ICT Sub-Portfolios

<table>
<thead>
<tr>
<th>Sub-Portfolio</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Intelligence** | - All ICT activities that wholly support functionality of an Intelligence line of business or business process, excluding DRN and DSN ICT infrastructure and common services  
- Manages the entire ICT requirements for the Intelligence Sub-Portfolio |
| **Military** | - All activities supporting Military ICT/Communication Information Systems (CIS) capabilities, excluding platform/weapon/sensor internal embedded systems  
- ICT/CIS that directly supports the functionality of a Military line of business or business process, excluding ICT/CIS infrastructure, common ICT services and includes Logistics Services  
- Manages the entire ICT requirements for the Military Sub-Portfolio |
| **Corporate** | - All ICT activities that wholly support the functionality of a Corporate line of business or business process  
- Manages the entire ICT requirements for the Corporate Sub-Portfolio |
| **Infrastructure** | - All ICT infrastructure that supports delivery of the functional services, such as applications or business processes  
- Manages the entire ICT requirements for the Infrastructure Sub-Portfolio  
- This Sub-Portfolio provides universally applicable (common) services that span Sub-Portfolios. It will supply reusable service components to enable a Service Oriented Architecture in pursuit of agility, interoperability and cost efficiency. The Chief Technology Officer Division will develop reference models and governance arrangements to support this approach  
- Common ICT assets such as data centre facilities, wide area networks, servers, workplace systems, storage, archival facilities, and systems that enable ICT operations  
- This will include common ICT services like email or identity management as well as those associated with business owners like finance and payroll |

**Prioritise for Effective ICT Spend**

Each Sub-Portfolio Committee will be given responsibility for managing priorities and requirements within their area. Each Sub-Portfolio Committee will consist of a membership of relevant stakeholders who represent ‘the voice of the customer’. The governance structure and Sub-Portfolio Committee membership is outlined in Figure Two. It is expected this membership will be refined throughout the course of implementation.
Optimise Project and Operations Efficiency

Defence will introduce mechanisms to ensure ICT resources and efforts are directed towards the priorities determined by the DICTC. This will include formalised practices and processes to:

- measure the time, budget and resources spent on ICT capability
- drive and monitor ongoing efficiency improvements
- ensure agreed priorities are delivered within scope, on time and under budget to meet required business outcomes

In keeping with Defence’s adoption of ‘Lean’ business practice core business processes will be examined with a view to eliminating unnecessary work, reducing the number of low value-adding tasks, and streamlining and automating workflows where possible. This will include increasing the use of shared services in areas such as payroll, HR, procurement and financial services. Defence will also adopt the Information Technology Infrastructure Library (ITIL) framework to streamline its processes in line with industry best practice.

Harmonise with Whole-of-government Initiatives

Defence will leverage off and align to other initiatives across government that shape ICT capability. Defence’s formal response to the Gershon Review of whole-of-government ICT outlines more detailed initiatives that will be undertaken as part of this strategy. Examples include the conversion of many professional service provider positions to Australian Public Service positions and Defence’s alignment with Gershon’s recommended governance structures.
Key Benefits

This strategic imperative will:

- Remedy the existing fragmented approach to Defence’s $1.2 billion annual ICT expenditure
- Manage demand by taking a portfolio management approach to ICT investment
- Establish appropriate governance mechanisms to make it possible for Defence to make enterprise-wide decisions on where ICT investment will yield the highest return
- Ensure adequate ICT investment in corporate and infrastructure services which are areas in need of attention due to previous underinvestment

Through the Sub-Portfolio Committees, Defence will be equipped with a stakeholder led approach to prioritising ICT, helping Defence direct ICT resources towards business priorities.
Strategic Imperative Two: Closer Stakeholder Engagement and Alignment

Strategic Imperative Two will enhance communication between Defence’s ICT capability providers and end users. It will also increase awareness of the ICT services required and consumed across Defence.

With this imperative, Defence is migrating to a stakeholder-aligned organisation model designed to improve understanding of stakeholder business needs, and improve engagement and collaboration, especially in regard to problem-solving.

This imperative will be addressed using five elements:

- Improve alignment between stakeholder needs and ICT capabilities
- Align ICT organisation with stakeholders
- Become easier to work with
- Design solutions collaboratively with stakeholders
- Implement Defence-wide ICT Governance

Improve Alignment Between Stakeholder Needs and ICT Capabilities

A stakeholder engagement team (SET) has been assigned to each of the Sub-Portfolios and is responsible for translating the priorities and requirements raised by stakeholders into business requests. The SETs will improve relationships with stakeholders through a strong end-user focus in the planning, delivery and operations areas of Defence ICT.

The SETs will leverage appropriate expertise to identify ICT solutions that allow for functional, technical, resource and timing factors while meeting the end-user needs. The SETs will seek to leverage existing capability where appropriate to minimise duplication. The structure and roles of the SETs are outlined below:

- Account Executive: responsible for oversight of all activities within the respective Sub Portfolio
- SET Desk Officers: working to the Account Executive the SET Desk Officers are responsible for engagement with stakeholders and for dealing with the prioritisation and progression of ICT outcomes
- Enterprise Architect: ensures all activities utilise current capabilities, conform, where applicable, to the Enterprise Architecture, and ensure the Sub-Portfolio can leverage emerging technology
- Development Executive: responsible for overseeing all enterprise wide development activities, raising solutions to off-track projects, and ensuring development effort for all options being assessed is understood; and for providing a communication channel between projects and stakeholders to maximise understanding by all parties of delivery related issues, constraints and priorities
- Service Executive: responsible for overseeing delivery of all standard ICT services within the respective Sub-Portfolios and ensuring the impact to Defence ICT of new requirements being considered is understood

Figure Four: Stakeholder Engagement Team 'Diamond' Structure

Each SET will be responsible for overseeing all ICT activities within its Sub-Portfolio. This includes:

- Maintaining an understanding of all proposed or scheduled projects
- Coordinating development of solution options to meet emerging stakeholder needs
- Facilitating the identification and implementation of enterprise wide solutions
- Overseeing development, operations and maintenance activities; and
- Assisting the Sub-Portfolio in prioritising requirements
**Portfolio Management Office**

The Portfolio Management Office (PMO) will provide administrative and process support to enable visibility and prioritisation of ICT business requests submitted through the SETs, thereby providing an aggregate view of Defence’s ICT Work Plan. This Work Plan will be reviewed by ICT providers and stakeholders, including the Sub-Portfolio Committees and the DICTC to ensure transparency and to ensure stakeholder-led priority setting. The relationship between the SETs and the PMO is outlined in Figure Five.

**Figure Five: Portfolio Management Office and Stakeholder Engagement Teams**
Aligning ICT Organisation with Stakeholders

The section below includes an explanation of the organisational model which Defence will use to plan, build, run and govern its ICT capability. The model brings together many of the themes and concepts discussed above, including portfolio management, Sub-Portfolios, SETs, PMO and the DICTC. Defence’s ICT Organisational Model is illustrated in Figure Six.

Figure Six: ICT Organisational Model
Organisational Model Explained

The ‘horizontal’ bars in Figure Six illustrate all Defence ICT resources and capabilities aligning to a plan, build, run or govern role. This model does not suggest that all Defence ICT resources will physically migrate to CIO group. This is a whole-of-Defence model and although some restructuring will occur the scale and complexity of Defence ICT is too great to consolidate into one group. Greater detail is outlined under Defence’s SRP and examples include the Fleet Information System Support Organisation role of the Navy migrating to CIO, and internal consolidation of I&S’s intelligence capability.

The model reinforces key Defence Management Review (DMR) and Defence Business Model principles such as the CIO performing the Coordinating Capability Manager role for ICT and having single technical authority over Defence’s entire ICT environment. More detail on how this will be achieved is covered under Strategic Imperative Three.

The ‘vertical’ bars illustrate the Intelligence, Military and Corporate Sub-Portfolios. Business requirements will be prioritised and agreed at the DICTC across the whole Defence ICT portfolio. The requirements of each Sub-Portfolio will be converted into business requests by the SETs.

The Infrastructure portfolio, representing the needs common to all areas of Defence (e.g. network and storage capacity) will largely be guided by an enterprise architectural plan managed by the CIO as part of the capability manager and single technical authority obligations.

Stakeholder business requests will be prioritised and consolidated into an enterprise ICT Work Plan by the PMO. All of Defence’s ICT resources with ICT plan, build, run and govern roles will ultimately align to this Work Plan which will be aligned to Defence’s business objectives.

Become Easier to Work With

Future state Defence ICT will realign processes, especially around help desk and service support, to ensure end-user experience is improved. Consolidation and centralisation of ICT services will lead to faster access to appropriate service desks, more accurate issue escalation, and decreased hold times. Defence will adopt best-practice frameworks such as the ITIL to assist with these improvements.
Design Solutions Collaboratively with Stakeholders

The majority of this strategy will be achieved through standing up the Intelligence, Military, and Corporate SETs to ensure solutions are provided for stakeholders’ needs. The Sub-Portfolio Committees will provide the mechanism for raising and prioritising work within the Sub-Portfolios and for ensuring requirements align to business needs. The Sub-Portfolios will also be an integral part of a more efficient approach to the delivery of ICT projects. An enterprise solutions approach will see collaboration across Defence in the definition and analysis of capability requirements within a common framework. This will provide stronger oversight and increased accountability during the solution design stage of ICT projects, ensuring the most appropriate solutions are considered for all ICT investments.

The Infrastructure Sub-Portfolio will cater to the needs of all ICT users by assuring the capacity and interoperability of new and existing technology through Defence’s soon to be developed Integrated Defence Architecture (see also Strategic Imperative Three).

Implement Defence-wide ICT Governance

Successful execution of the proposed strategies relies upon Defence-wide management of the ICT portfolio. At a strategic level the DICTC provide the strategic and financial governance from a Defence-wide perspective, adjusting Sub-Portfolio budgets and activities as needed.

Technological and architectural standards (discussed further under Strategic Imperative Three) will provide opportunities for further cost savings and service effectiveness through standardisation and reuse of capability. An enterprise-wide architectural committee will be responsible for governance in this arena.

The SETs and Sub-Portfolio Committees provide the mechanism for more effective stakeholder engagement and provide greater assurance that ICT investment is targeted towards agreed business needs. The CIO will have overall accountability and single technical authority for Defence’s ICT capability, and will apply Defence’s ICT organisational model to engage and align ICT resources.
Key Benefits

This strategic imperative will:

- Improve Defence's ability to raise and prioritise ICT requirements and facilitate a stakeholder led approach via the Sub-Portfolio Committees
- Ensure stakeholder engagement teams provide the right expertise to generate business requests for stakeholder requirements, thereby addressing existing shortcomings that have seen ICT providers defining priorities and ICT users mandating technical solutions instead of the other way around
- An ICT enterprise Work Plan will provide greater transparency of Defence’s priorities and expenditure, collated by the PMO
- Improve visibility of priorities and resource availability to enable better management of demand for ICT services and products across Defence

Figure Seven: ICT Governance and Direction
Strategic Imperative Three: Provide Agreed, Priority Solutions

Strategic Imperative Three will encourage the development and use of common and standardised services, reduce duplication of technology investments and deliver solutions which meet prioritised business requirements.

...encourages the development and use of common and standardised services

Achieving Strategic Imperative Three relies upon delivering five strategic elements:

- Stabilise and secure ICT
- Consolidate, standardise and optimise ICT
- Address new ICT requirements
- Leverage emerging technologies to address new business needs
- Create and adopt an Enterprise Architecture

Stabilise and Secure ICT

Stabilising and securing ICT will assure the availability of services and increase the stability of Defence's ICT at both fixed and deployed locations.

Through a single interface Defence will secure its Information Environment and deliver authorised users access to the information and services they need. It will enable secure collaboration among allies and coalition partners, delivering a highly available network to support prioritised operations and instil confidence in the ability to synchronise information and make strategic decisions.

Defence will also secure its ICT by:

- Providing updated security policy, procedures and plans
- Providing training for staff in security-related roles
- Developing the security layer of the Integrated Defence Architecture (IDA, see Figure Eight)
- Introducing an effective security risk management system
- Maintaining regular updates to security threat and risk assessments
- Conducting strengthened certification and accreditation
- Remediating the current non-compliances with mandatory requirements of ACSI-33 and the Defence Security Manual
- Investing in Computer Network Defence capabilities
**Consolidate, Standardise and Optimise ICT**

Consolidating, standardising and optimising ICT will reduce the complexity and duplication within the Defence Information Environment whilst also increasing the efficiency and effectiveness of Defence’s ICT capabilities and services.

Defence will seek to standardise its ICT infrastructure investments through virtualisation, rationalisation of the application portfolio and through the standardisation of supported technology and product platforms.

The IDA will assist in driving the standardisation of ICT within Intelligence, Military, Corporate and Infrastructure portfolios. Defence will also focus on the consolidation of data centres and associated infrastructure in the short-term.

These efforts will be consistent with the whole-of-government approach for data centre requirements over the next 10 to 15 years which will also take into account key factors such as disaster recovery, growth in space requirements and geographic location.

**Addressing New ICT Requirements**

New ICT requirements will be addressed through regular communication and engagement by the newly formed stakeholder engagement teams as discussed in Strategic Imperative Two.

This approach will ensure that new ICT requirements will be captured and aligned with the existing capabilities and design of the IDA. The IDA will also support the incorporation of new ICT requirements through its flexibility and adaptability. This will be achieved through the IDA’s service-oriented architecture backbone and by adherence to the following key design principles:

1. Integrated architecture: Connection and integration of Defence’s various operating models and business domains and ICT alignment through an enterprise architecture supporting Intelligence, Military, Corporate and Infrastructure portfolios
2. Information as an enterprise asset: Support the management of information and data to enable effective decision making, collaboration and interoperability ensuring reliability, integrity and trust worthiness
3. Business service-orientation: Flexibility and modularity to cope with evolving business needs and support efficient delivery of business services which are either common across the enterprise, standardised within one or more portfolios, or specialised within a specific portfolio or domain as described in the NCW Roadmap 2009 (Fig 3-1 NCW milestones and the domain construct).
4. Effective return-on-investment of ICT: Enable effective investment and management of ICT by capturing and realising the business value of ICT and linking these to Defence’s strategic business outcomes.

Through this approach Defence will also be able to respond to new ICT requirements such as ‘Green-IT’. This mechanism will ensure that Defence can align with a future whole-of-government ICT sustainability plan to better manage the carbon footprint of government ICT activities.
Leverage Emerging Technologies to Address New Business Needs

Defence will leverage and embrace emerging technologies to address new business needs through the development of strategic technology roadmaps and through the adoption of prudent technology lifecycle management practices.

Create and Adopt an Enterprise Architecture

The creation and adoption of an enterprise architecture is the foundation of Strategic Imperative Three. The IDA has been developed as a means for Defence to guide and align future investment decisions and for the strategic planning of information technology and systems. The IDA, illustrated in Figure Eight, provides:

1. A conceptual view of the future state or target architecture for the Defence enterprise
2. A common medium for communication and planning between Defence business and ICT
3. Multiple perspectives of the Defence enterprise including performance, business, services, data and technology
4. Relationships and dependencies both horizontally (i.e. within a single perspective of the architecture - what data is shared or self-contained) and vertically (i.e. across multiple perspectives of the architecture - what business functions and processes are supported by what systems/services)
5. Key insight to enable strategic decisions and planning
Defence will seek to review and frame the major programs in the Defence Capability Plan that either impact or rely on ICT in order to provide strategic direction, guidance and alignment. Defence will focus initially on the design and delivery of the following three high priority architecture improvement initiatives:

1. Building and delivering the target architecture or IDA
2. Integrating, securing and enhancing the network
3. Managing information as an asset
The CIO will oversee the design of the IDA and has established a Chief Technology Officer (CTO) Division to drive stewardship and direction of the IDA. Creating an effective CTO organisation within Defence ICT provides a basis for setting the overall architectural direction of the IDA to align strategic decisions and ensures that ICT needs and enterprise challenges across Defence are considered holistically as discussed in Figure Nine.

Figure Nine: CTO Support to Address Current-state Enterprise Challenges

<table>
<thead>
<tr>
<th>Enterprise Challenges</th>
<th>CTO Support to Address Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Stove-piped processes and IT solutions</td>
<td>- Establishes a ‘line of sight’ of the contribution of IT to mission and program performance</td>
</tr>
<tr>
<td>- Highly complex system of applications, hardware platforms, and operating systems</td>
<td>- Facilitates the identification of consolidation opportunities around common or similar</td>
</tr>
<tr>
<td>- Unwanted redundancy in applications and data to support the business</td>
<td>performance objectives, Defence functions, and data and information</td>
</tr>
<tr>
<td>- High acquisition costs and risks associated with new systems development and technology</td>
<td>- Creates a common language and library for discussing Defence and IT</td>
</tr>
<tr>
<td>- Inability to associate IT costs with services to the Defence units or stakeholders</td>
<td>- Provided insight into available IT assets, how much they cost, and who is using them</td>
</tr>
<tr>
<td>- Defence units unaware of available services</td>
<td>- Provides a blueprint to support the acquisition or development of future IT systems</td>
</tr>
<tr>
<td>- Multiple, often inconsistent data sources</td>
<td>- Formulates and applies enterprise-wide IT standards and processes</td>
</tr>
<tr>
<td>- Uncertain business ownership of IT assets</td>
<td>- Provides accurate data for IT investment, capital allocation, and other governance decisions</td>
</tr>
<tr>
<td>- Limited ability to implement systems rationalisation or take other efficiency-creating actions</td>
<td>- Installs technology roadmap as framework for future application requirements</td>
</tr>
<tr>
<td>- Defence units uncertain of how to initiate or follow IT projects</td>
<td>- Enables business-driven approach to IT decision making</td>
</tr>
<tr>
<td>- Lack of communication between Defence and IT</td>
<td></td>
</tr>
<tr>
<td>- Gaps in technology support to Defence</td>
<td></td>
</tr>
</tbody>
</table>

The establishment of the CTO Division is a key enabler to Defence’s CIO maintaining single technical authority. The IDA is the mechanism that will be used to plan for and capture the key technical decisions that impact Defence’s ICT capability.

Enterprise Solutions

Defence will adopt an enterprise-solutions approach to the planning and delivery of ICT projects. This will help Defence to dramatically improve the quality, throughput and economic performance of ICT programs and operations. The Chief Information Officer has established a Defence ICT Enterprise Solutions Branch to be a centre of excellence within the following areas.

1. The translation of business needs into a standard set of specifications that define functional and non functional requirements.
2. Assessment of specifications that define the most efficient and effective ICT solution available to Defence. Solution options will include both the procurement of new systems and, importantly, the maximum utilisation of existing technologies regardless of origin. Solutions will also be based on transparency of whole-of-life cost and support issues.
3. Defence will develop and maintain operating procedures to effectively manage the solution integrity during the complete delivery cycle, ensuring alignment to business needs are maintained through traceable change management practices.

**Key Benefits**

The specific benefits delivered through Strategic Imperative Three include:

- improved agility of solution delivery across both fixed and deployed locations
- minimised duplication of platforms and systems through consolidation, resulting in cost-savings and efficiency gains
- clarity on ‘how things work’ and mission criticality of business processes, improving business continuity and operational resilience
- improved ICT capability through the delivery of common and standardised services across the Defence enterprise
- improved interoperability across Defence and with key allied and coalition partners, industry and whole-of-government
- more effective ICT investment decisions, program planning and delivery and business-ICT alignment
Strategic Imperative Four: Strengthen ICT Capability

Strategic Imperative Four will strengthen the organisation's culture, skills, processes and practices to support development of ICT capability.

This is achieved through the following six strategic elements:

- Energise the culture
- Strengthen ICT leadership
- Improve processes and tools
- Professionalise the workforce
- Leverage vendors and sourcing
- Leverage scale and effective resource planning and management

Energise the Culture

To successfully execute the ICT strategy, Defence ICT will need to develop a stakeholder-focused culture underpinned by effective communication. To address this need, Defence ICT will implement a people change program that focuses on the core components illustrated in Figure 10.

Figure 10: People Change Approach
Defence ICT will place an emphasis on three components of HR:

- Recruitment/assessment and selection
- Performance management
- Learning, development and retention

**Strengthen ICT Leadership**

Defence will develop a leadership team that is empowered to deliver the strategic imperatives essential to build ICT capability across the whole-of-Defence. Figure 11 illustrates that ICT capability has direct links to leadership, strategic imperatives and the ICT community.

As captured in Defence's ICT organisation model, many key positions are crucial to the future state of Defence's ICT. Examples include the DICTC, Sub-Portfolio Committees, SETs and leaders in the plan, build, run and govern space. Defence is committed to providing capable and accountable leadership in these positions to drive progress.

Figure 11: Factors to Strengthen ICT Leadership
Improve Processes and Tools

Defence will implement a new process to support governance of ICT projects. This process will allow faster approvals of projects, where cost, risk and complexity do not preclude this. Specific process improvements will include, but not be limited to:

- The development of faster and more agile ICT investment processes that are more responsive to the short timeframes for ICT platforms
- Improved project prioritisation and approval processes based on Sub-Portfolios that allow business stakeholders to drive prioritisation decisions
- An annual Sub-Portfolio planning process that establishes a forward plan of project activity to align ICT plans with business demand and support more effective operation of ICT
- Consistently implementing delivery process improvement frameworks and standardisation of project delivery methodology

Moving to a Shared-Services Model

Defence will make the necessary ICT investments required to deliver the centralisation and standardisation of ICT service delivery and a continuation of the move to shared services. This will achieve operating efficiencies in support of future capability requirements.

The shared services model is expected to encompass reform to the delivery of services such as:

- Communication services
- Hosting and data services
- Network services
- Client devices
- ICT user support
- Application services
- Database services

Professionalise the Workforce

Defence has a substantial ICT workforce and needs to continually attract and retain skilled staff. One key driver of job satisfaction for ICT professionals is professional career progression and growth in ICT skills. Defence will establish communities of practice to drive a focus on professional career progression and skills growth and to provide a stronger alternative to the existing managerial career progression options.

Through communities of practice, Defence ICT will drive a greater consistency in functional skills sets across Defence ICT and propagate widespread use of leading practices. Further, the communities will establish standard approaches for skill development, certification and professional development. Professional networks are fostered through greater awareness of other peer professionals, visibility of innovation, and an understanding of current issues faced by other professionals.
Workforce Planning

ICT workforce planning across Defence will be consolidated. Changes introduced as part of the ICT reform program will deliver improved Defence ICT career-path management and workforce planning. In particular, it will optimise the workforce profile mix between APS, ADF and contractors.

Taking a whole-of-Defence approach to the management of ICT personnel will also deliver to Defence the flexibility to reassign this valuable resource across the portfolio as our ICT priorities change.

Figure 12: Communities of Practice
Leverage Vendors and Sourcing

Defence ICT is a major consumer of ICT goods and services and this scale as a consumer is a lever that is currently under utilised. To drive improved sourcing outcomes and better leverage the capability of ICT vendors, Defence will implement a ‘Procurement Centre of Excellence’. The ‘Procurement Centre of Excellence’ will have a remit to establish strong common ICT procurement processes and deliver improved outcomes from sourcing activity.

The ‘Procurement Centre of Excellence’ will complete the ICT Sourcing Strategy which will include:

- Identification and classification of contract related costs associated with the delivery of ICT services
- A review of service delivery costs and sourcing models against industry and whole-of-government metrics to define the sourcing opportunities within the Defence ICT value chain
- Establishing strategic ICT sourcing principles that are linked to stakeholder needs and Defence’s ICT strategy to guide the sourcing strategy
- Definition of a technology bundling strategy based on the ICT sourcing principles, overall procurement cost, vendor specialisation and economies of scale
- Linkage of the Defence ICT sourcing strategy with whole-of-government initiatives
- Continued development of the internal sourcing communication strategy to increase knowledge of ICT procurement guidelines and policies among all staff involved in Defence ICT procurement

Defence will rationalise the vendor set to establish a manageable set of vendors involving fewer but more strategic partnerships. Current contract management within Defence ICT can be characterised as being focused on inputs. Defence will focus contract management on the delivery of business outcomes.

This function will review and improve contracts to ensure they are strongly performance-oriented with enforceable legal clauses. There will be a preference for milestone-based payment models. Further, vendors will be held accountable for delivery of outcomes by establishing risk sharing arrangement where appropriate.
Effective Resource Planning and Management

Defence has one of the largest ICT workforces in Australia but can currently be characterised as operating as many small ICT workforces. Defence can improve ICT outcomes and strengthen ICT capabilities by leveraging the scale of the Defence ICT workforce. Defence will establish an effective resource management system that provides visibility of ICT staff, staff availability and staff skills.

There is a strategic risk for Defence ICT centred on access to the right ICT staff within the Canberra market. To address this, Defence will establish an ICT Regionalisation Program. This ICT Regionalisation Program will establish one or more ICT project delivery, operations and/or maintenance facilities outside of the Canberra ICT skills market.
ADF members, who have communication and CIS responsibilities, represent a key ICT resource. Defence must refine and formalise the ongoing training and integration of ADF members into ICT communities of practice. This integration should include supporting their participation in skills management processes, their involvement in the ICT Regionalisation Program and their participation in ICT professionalism initiatives.

**Key Benefits**

The specific benefits delivered through Strategic Imperative Four include:

- Improved focus on a culture of effective stakeholder engagement and delivery of services
- Clarity of expectations of role and responsibilities in relation to delivery of ICT capability consistent with organisational priorities and expectations
- Improved delivery of professional, effective and efficient ICT services, consistent with identified better practice and industry standards, to Defence
Outcomes and Benefits of this Strategy

This ICT Strategy will improve efficiency and effectiveness within Defence’s ICT portfolio. In doing so, it will help Defence achieve its mission of defending Australia and its interests. The ICT Strategy will enhance ICT capabilities and drive the following five outcomes to address Defence’s business needs.

Greater ICT Scalability, Flexibility and Adaptability

Defence will increase its ICT capability to support a growing number of simultaneous operations. Defence will improve its flexibility to support operations in which force composition may not be known in advance. This will be achieved through enhanced information management and via the stakeholder engagement teams and their ability to facilitate improved decision-making regarding ICT requirements.

Defence will improve access to, and delivery of, ICT services for ADF operations conducted in areas with no fixed infrastructure. Defence will also enable ICT support for increasing numbers of non-Defence staff in operational areas through its ‘deployed architecture’ pattern as part of the Integrated Defence Architecture (IDA) and its strengthened ICT support capability.

Improved Information Speed and Accuracy

Defence will improve the speed of access to information across all internal sources including the extended enterprise (i.e. allies, coalition partners and whole-of-government) via its information management strategy and through its ‘managing information as an asset’ architecture improvement initiative. The ‘integrating, securing and enhancing the network architecture’ initiative will further enhance collaboration and information connectivity.

Defence will implement more rigorous ICT service management such as ICT asset, configuration, capacity and demand management; and service measurement processes. This will provide the baseline from which to make the investments needed to manage a significant increase in the coverage of the battle-space (visual, radio frequency, infra-red, radar, etc.) and to move to an increased focus on real-time data (i.e., sensor to shooter).

Continued Technological Capability Edge

Defence will maintain a technological capability edge over its adversaries through enhanced computer and network capabilities, and by integrating, securing and enhancing the network architecture, with a focus on information assurance, confidentiality, integrity and availability of Defence’s information and infrastructure.

Defence will also maintain a capability advantage in traditional areas such as sensors, combat systems, communications, unmanned vehicles, etc. as well as emerging areas such as telemedicine and simulation.
Enhanced Interoperability

Defence will build its ICT interoperability capabilities to support inter-agency collaboration and engagement with coalition partners in conducting operations.

Through the IDA, Defence will foster the use of common and standardised business services and will reduce duplication and proliferation of ICT investments throughout the environment.

Improved Business Support

ICT support to Defence business will be improved by holistically managing the ICT environment. The process standardisation initiatives and tools will deliver clear processes for executing ICT work, including management of the ICT portfolio as a whole.

The establishment of stakeholder engagement teams, demand planning, customer feedback mechanisms, customer experience measurement tools will provide better engagement with Defence stakeholders, an increased focus on customer satisfaction in ICT, key performance indicators, and a single service desk process and tool set will improve business support.
Implementing our ICT Strategy

All strategies are only as valuable as their translation into action. A significant portion of this strategy will be implemented within two to three years via multiple parallel programs. Some programs will persist beyond that time; developing and improving the delivery of ICT capabilities.

It is important to recognise that the ICT initiatives outlined in this strategy will be implemented and prioritised as components of the Defence SRP. These ICT initiatives cannot be delivered in isolation and will be sequenced to enable Defence business process reform.

Implementation of this strategy will need significant Defence-wide collaboration to ensure the new organisation structure both aligns to stakeholder needs and allows the CIO to act as the Coordinating Capability Manager for all ICT in Defence.

An important premise of this strategy is that existing ICT resources and projects will be used to the maximum extent possible, reducing both costs and reliance upon external providers.

Several critical deliverables will be implemented over the short term. These include:

- Standing up the SETs to help prioritise requirements
- Standing up the new matrix organisation structure to support the SETs
- Deploying the refined portfolio management process to manage the approval, and monitor the delivery and ongoing sustainment of ICT capabilities

A strong and rigorous governance structure will help support, monitor and manage the implementation. The Defence Executive, under new governance arrangements (see ICT Governance and Direction, Figure Seven) will continue to monitor and assess risks as they are identified.

An external review committee will also monitor implementation of reform under the wider Defence SRP. The Defence Strategic Reform Advisory Board will report to the Minister for Defence quarterly, who will in turn report to the National Security Committee of Cabinet annually on progress of Defence reforms. The key function of the Board will be to provide advice on how the reforms should be implemented, and assist in ensuring the reforms are being implemented in the way intended by government.

ICT Reform Program

The Defence ICT Reform Program will be the principle vehicle for the management and delivery of the Defence ICT Strategy. The ICT Reform Program will build an improved DIE and governance framework that can effectively support Defence war fighting and business reform objectives through to 2030.
The key outcomes of the reform program include:

- Improved alignment of ICT investment with Defence priorities by adopting a single portfolio of ICT investments for all parts of Defence
- Reducing the high ‘business as usual’ costs through tighter control, new sourcing strategies and standardising and consolidating ICT assets across all parts of Defence
- Implementing faster decision and delivery cycles to reduce costs and ‘time to market’
- Addressing the long-term underinvestment in ICT infrastructure that has resulted in a significant proportion of assets being beyond their effective life and mitigating an unacceptable business risk
- New investments to enhance our networks and information management capabilities to support better decision-making across Defence
- Consolidating infrastructure to reduce maintenance costs and prepare Defence to reduce its carbon footprint
- Implementing a more responsive stakeholder engagement model

This program will ensure that while ICT continues to meet the immediate needs of the military operations there is also a dedicated management team focussing on longer-term business reform.

**ICT Work Plan**

All of the initiatives implemented as part of this strategy will be managed as components of a single Defence ICT Work Plan under the ICT Reform Stream. The Chief Operating Officer is responsible for maintaining the Defence ICT Work Plan under the wider governance arrangements outlined earlier in this strategy and will lead the ICT Reform Program Office.

The following are some of the initiatives that Defence will undertake as part of the implementation of this ICT strategy. The selected initiatives are categorised according to the Strategic Imperatives of this strategy.
Implementing Strategic Imperative One: Optimise Defence ICT Investment

Initiative: Consolidate Data Centres

The DIE Data Centre Strategy will provide an ICT framework to support the ADFs operational and support organisations for the next 10 years. To meet the demands of the ADF, the strategy must enable reliable, flexible and sustained delivery of information services in line with Defence’s requirements.

The DIE currently supports 200 data centre/server rooms. The cost of supporting these facilities is difficult to quantify, however it appears Defence has under-estimated, under-resourced and under-planned its data centre capability in the past. Defence is now addressing this under-investment and developing a coherent capability able to support both current and expected demand. This is being done cognisant of whole-of-government data centre standardisation efforts.

With a defined data centre strategy and consolidation program the number of facilities can be reduced considerably.

Initiative: Reduce ‘Time to Market’ ICT Two Pass Process

This initiative will include a review of the approval processes used for Defence-wide ICT investments with the aim of introducing an alternative framework to compress decision and delivery cycles. The current processes through which Defence ICT capability is procured are lengthy and cannot keep pace with the speed of new technology development, leading to the unacceptable risk of delivering obsolete technology.

The new approvals framework for Defence-wide ICT investments will be modelled on successful commercial practices and the whole-of-government ICT Two Pass process.

Initiative: Implement a Single Secure Desktop

The Single Desktop Program will de-clutter the desktops of Defence personnel. Currently those personnel who need to access multiple networks, such as the Restricted network and the Secret network, need multiple computers on their desk.

This Program will see these units replaced with a single system that provides access to multiple networks via a solution using a combination of hardware and software. It will result in the introduction of multi-level information-sharing across security domains.
Initiative: Develop Defence’s Enterprise Architecting Capabilities

Developing Defence’s enterprise architecting capabilities will provide the means for aligning Defence capability and outputs with Defence’s strategic drivers. The development of the Defence enterprise architecting capability will focus on:

- Establishing a capable Chief Technology Officer Division
- Enhancing the current Defence Architecture Framework (DAF)
- Implementing supporting strategic and technical control frameworks
- Establishing and maintaining an integrated view of Defence’s architectural direction to provide a common medium for communications between the business and ICT whilst guiding strategic decisions and planning

Initiative: Implementing a Services Oriented Architecture

The implementation of a Defence wide Services Oriented Architecture (SOA) infrastructure will drive efficiency without compromising effectiveness across Defence by delivering reusable, granular, modular and interoperable services. This will enable Defence to introduce more centralised and standardised support services and processes that make greater use of e-business solutions built on a SOA infrastructure.

This initiative will deliver the policies, processes, skills, tools and fundamental capabilities for the implementation of a multi-domain Defence wide SOA infrastructure based on the current Defence e-Business Infrastructure (DeBI), and Defence Online Services Domain (DOSD).

Initiative: DIE Simulation and Modelling

Simulation and modelling can help to drive down costs, reduce risk and enhance capability. Defence will make greater use of simulation for these reasons; the architecture of the future DIE will support this. In addition, modelling and simulation will increasingly be applied to the management of Defence ICT.

Initiative: Centralised Services - Deliver Distributed Computing

The Central Services Program will improve the management of those services that can be delivered remotely from a central location over the Defence Restricted, Defence Secret and Defence Top Secret networks. This includes service desk services, and managing and monitoring of hardware and deployment of software updates.
Implementing Strategic Imperative Two: Closer Stakeholder Engagement & Alignment

Initiative: New Stakeholder Engagement Model

CIO is establishing SETs to improve interaction with Services and Groups. Three SETs: Intelligence, Military and Corporate will work across the portfolios. Infrastructure will be handled as a separate portfolio of activity by the CIO Chief Technology Officer.

CIO is also working with Services and Groups to facilitate and improve their ability to prioritise ICT requirements via their respective ICT group points of contact and the soon to be established ICT Sub-Portfolio Committees.

Initiative: Improved Sharing and Access to Services with Key Allies

The Interoperability Improvement Plan aims to improve connectivity and information sharing that supports the planning and conduct of combined operations and Defence business activities.

Initiative: Specialist Business Solutions Design Capability

This function will provide a more integrated and interoperable solutions-design capability with faster decision cycles. This will ensure that technical solutions meet the user requirements as defined by the SETs and supporting business cases.

Implementing Strategic Imperative Three: Provide Agreed, Priority Solutions

Initiative: Information Management

Effective information management will provide a competitive advantage in situational awareness, rapid decision making and the precise application of force over our adversaries. In addition, effective information management will ensure that costs associated with military capability are reduced by eliminating ‘stove-piping’ of information and ensuring that the principle of ‘need to share’ (within security constraints) becomes pervasive.

This initiative will provide the ability to support the entire information management life cycle. This will be achieved by developing and implementing information management processes, policies, skills, technologies and procedures Defence wide.
Initiative: Deliver Unified Communications

Unified Communications (UC) includes such capabilities as instant text messaging, voice calls, video calls, application sharing, presence, and call recording using a common platform.

The Defence Secret Network Unified Communications (DSN UC) Project will deliver the primary means by which users within the DSN will electronically communicate via voice. The DSN UC Project will be capable of scaling to meet the needs of all DSN users.

Initiative: High Speed Strategic Communications Network (JP 2047)

This initiative will help Defence improve the conduct of operations and the management of its business. It will deliver a high-speed Defence Strategic Communications Network that will include the wide area network and base area networks in Australia, as well as links with selected fixed overseas sites, and interfaces to military communications and external partners.

Initiative: Analysis of Disruptive Technology

Defence will apply its research, intelligence and modelling capabilities to assess the ICT capability risks and opportunities of potentially disruptive technologies - and use these assessments in support of strategic and architectural decision making. The Chief Technology Officer Division will include a technology futures function to provide coordination.

Implementing Strategic Imperative Four: Strengthen ICT Capability

Initiative: Sourcing Strategy

Although most of CIO’s ICT spend is external, it is not strategically managed:

- 85 per cent of expenditure is spent on external providers yet sourcing is highly fragmented, and procurement is decentralised and uncoordinated
- Existing contracts focus on inputs rather than end-to-end accountabilities for business outcomes
- Sourcing acts as a bottleneck, hindering the delivery of business outcomes

Defence plans to have more strategic relationships with fewer vendors. In doing so Defence will consolidate infrastructure sourcing into five bundles: distributed computing, centralised processing, terrestrial communications, specialist communications and applications.

The scope of the ICT sourcing program will deliver new sourcing arrangements that will bundle the delivery of ICT services so that Defence reaps significant cost savings as well as offering the opportunity to free up staff from procurement and governance duties.
Initiative: Investing in People

The strategic workforce plan will form the basis for ongoing whole-of-government ICT workforce planning. It will detail the current capacity and capability of the APS ICT workforce, identify the anticipated changes in the short to medium term, and outline the shifts in capability and capacity required for the future effective and efficient achievement of government’s priorities. Additionally, the plan will provide broad direction at the whole-of-government level on how to improve the recruitment, retention and engagement of ICT personnel.

Initiative: IT Service Management

IT Service Management (ITSM) is a discipline for managing IT systems focused on the customer’s perspective of IT’s contribution to business. ITSM stands in deliberate contrast to technology-centric approaches to IT management and business interaction.

The ITSM Project within Defence will implement:

- One corporate set of ICT service management processes for interaction, incident, problem, change and release management based on ITIL v3 best practices
- A central DSN, DRN and Voice self service web portal that allows all users to make their own requests through the corporate service catalogue and enquire on the status of their requests
- One corporate service catalogue that offers all ICT products and services in a logical way, regardless of which part of the organisation the owning ICT function operates in or is provisioned from
- A central DSN, DRN and Voice service desk toolset for use by all ICT service and support groups operating in these environments
- One central DSN, DRN and Voice federated CMDB (Configuration Management Database) that supports change impact analysis across all ICT assets

The ITSM Project will also decommission all existing DSN and DRN ICT service management toolsets as each service and support group is transitioned to this new corporate capability.

Initiative: ICT Reform Portfolio Management

The ICT Reform Portfolio Management Office will coordinate, integrate and provide oversight of all ICT Reform activities. In doing so, it will provide governance and alignment to ensure the delivery and success of the Defence SRP outcomes.

- Define the change methodology - aligned with broader SRP
- Manage interdependencies between ICT and non-ICT reform streams
- Establish and enforce accountabilities especially with respect to delivering on savings targets and the timing of non-financial outcomes
- Manage program risks and issues
- Manage communication and information flows between ICT reform streams and provide the:
  - Single, independent source of truth in form of baselines and target architecture
  - Standardised methodologies
  - Common approach
Initiative: CIO as Coordinating Capability Manager

The Chief Information Officer has been made accountable for delivering the ICT capabilities required to support broader Defence SRP, delivering the target ICT operating model and architecture, and achieving the agreed ICT savings targets as the Coordinating Capability Manager for Defence ICT.

Initiative: Infrastructure Remediation

A program of activity has begun to address the risk posed by the advanced age of the Defence ICT fleet. This program will replace aging desktops, printers, laptops, monitors as well as PABX and other network equipment.

It will also include server, storage and backup remediation spread over the next two financial years, as well as the replacement of all known out-of-warranty switch and router infrastructure.

Enabling Defence Business Reform

In addition to the initiatives listed above, Defence will work collaboratively to introduce new capabilities such as the automation of procurement, personnel and pay administration, vetting, recruitment, estate management and management reporting.

Table Two: ICT Reform Timelines

<table>
<thead>
<tr>
<th>Activity</th>
<th>09-10</th>
<th>10-11</th>
<th>11-12</th>
<th>12-13</th>
<th>14-15</th>
<th>15-16</th>
<th>16-17</th>
<th>17-18</th>
<th>18-19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workforce</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diagnostic transform design</td>
<td></td>
<td></td>
<td>Begin civilianisation &amp; contractor conversion</td>
<td>Implement lean business processes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shared Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diagnostic transform design</td>
<td></td>
<td></td>
<td>Business process redesign &amp; implement &amp; support</td>
<td>Transformation to efficient &amp; effective IT enabled processes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information &amp; Communications Technology</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diagnostic transform design</td>
<td></td>
<td></td>
<td>Optimise value of Defence ICT provide agreed priority solutions</td>
<td>Strengthen ICT capability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No or <20% of mature yearly savings

20-50% of mature yearly savings

50-100% of mature yearly savings

100% of mature yearly savings
Table Three: Glossary, Abbreviations and Acronyms

<table>
<thead>
<tr>
<th>Term/Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACSI</td>
<td>Australian Communications Security Instruction</td>
</tr>
<tr>
<td>ADF</td>
<td>Australian Defence Force</td>
</tr>
<tr>
<td>AFP</td>
<td>Australian Federal Police</td>
</tr>
<tr>
<td>AGA</td>
<td>Australian Government Architecture</td>
</tr>
<tr>
<td>APS</td>
<td>Australian Public Service</td>
</tr>
<tr>
<td>ASIO</td>
<td>Australian Security Intelligence Organisation</td>
</tr>
<tr>
<td>C2</td>
<td>Command and Control</td>
</tr>
<tr>
<td>CA</td>
<td>Chief of Army</td>
</tr>
<tr>
<td>CAF</td>
<td>Chief of Air Force</td>
</tr>
<tr>
<td>CFO</td>
<td>Chief Finance Officer</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CIS</td>
<td>Communications and Information Systems</td>
</tr>
<tr>
<td>CJLOG</td>
<td>Chief Joint Logistics</td>
</tr>
<tr>
<td>CJOPS</td>
<td>Chief Joint Operations</td>
</tr>
<tr>
<td>CMDB</td>
<td>Configuration Management Database</td>
</tr>
<tr>
<td>CMMI</td>
<td>Capability Maturity Model Integration - Process improvement approach</td>
</tr>
<tr>
<td>CN</td>
<td>Chief of Navy</td>
</tr>
<tr>
<td>COO</td>
<td>Chief Operating Officer</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial off the Shelf</td>
</tr>
<tr>
<td>CSPC</td>
<td>Corporate Sub-Portfolio Committee - Committee specific to the Corporate stakeholder group</td>
</tr>
<tr>
<td>CTO</td>
<td>Chief Technology Officer</td>
</tr>
<tr>
<td>DAF</td>
<td>Defence Architecture Framework</td>
</tr>
<tr>
<td>DeBI</td>
<td>Defence e-Business Infrastructure</td>
</tr>
<tr>
<td>DGI&amp;S</td>
<td>Director General Intelligence &amp; Security</td>
</tr>
<tr>
<td>Term/Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>DICTC</td>
<td>Defence Information and Communications Technology Committee</td>
</tr>
<tr>
<td>DIE</td>
<td>Defence Information Environment</td>
</tr>
<tr>
<td>DMO</td>
<td>Defence Material Organisation</td>
</tr>
<tr>
<td>DMR</td>
<td>Defence Management Review</td>
</tr>
<tr>
<td>DNSA</td>
<td>Defence Network Support Agency</td>
</tr>
<tr>
<td>DOSD</td>
<td>Defence Online Services Domain</td>
</tr>
<tr>
<td>DRMS</td>
<td>Defence Record Management System</td>
</tr>
<tr>
<td>DRN</td>
<td>Defence Restricted Network</td>
</tr>
<tr>
<td>DSA</td>
<td>Defence Security Authority</td>
</tr>
<tr>
<td>DSG</td>
<td>Defence Support Group</td>
</tr>
<tr>
<td>DSN</td>
<td>Defence Secret Network</td>
</tr>
<tr>
<td>DSTO</td>
<td>Defence Science and Technology Organisation</td>
</tr>
<tr>
<td>DWACN</td>
<td>Defence Wide Area Communications Network</td>
</tr>
<tr>
<td>EA</td>
<td>Enterprise Architecture</td>
</tr>
<tr>
<td>ERP</td>
<td>Enterprise Resource Planning</td>
</tr>
<tr>
<td>ESP</td>
<td>External Service Providers</td>
</tr>
<tr>
<td>FASICTD</td>
<td>First Assistant Secretary Information and Communications Technology Development</td>
</tr>
<tr>
<td>Force 2030</td>
<td>A Defence strategic priority outlined in the 2009 Defence White Paper</td>
</tr>
<tr>
<td>FTE</td>
<td>Full-Time Equivalent</td>
</tr>
<tr>
<td>GDP</td>
<td>Gross Domestic Product</td>
</tr>
<tr>
<td>Gershon Report</td>
<td>Independent review commissioned by the Department of Finance and Deregulation of the Australian Governments use of ICT by Sir Peter Gershon</td>
</tr>
<tr>
<td>HICTO</td>
<td>Head Information and Communications Technology Operations Division</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resources</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>ICT Operations</td>
<td>ICT Operations is the provision of day-to-day technical supervision and administration of the ICT infrastructure. ICT Operations staff are responsible for providing a stable, secure ICT infrastructure, maintaining a current and up to date Operational Documentation Library (’ODL’), maintaining a log of all operational events, maintenance of operational monitoring and management tools, operational scripts and operational procedures such as job scheduling, backup and restore, and monitoring</td>
</tr>
<tr>
<td>Term/Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IDA</td>
<td>Integrated Defence Architecture - Future-state enterprise architecture for Defence</td>
</tr>
<tr>
<td>INFSPC</td>
<td>Infrastructure Sub-Portfolio Committee - Committee specific to the Infrastructure stakeholder group</td>
</tr>
<tr>
<td>I&amp;S</td>
<td>Intelligence and Security</td>
</tr>
<tr>
<td>ISPC</td>
<td>Intelligence Sub-Portfolio Committee - Committee specific to the Intelligence stakeholder group</td>
</tr>
<tr>
<td>ISR</td>
<td>Intelligence, Surveillance and Reconnaissance</td>
</tr>
<tr>
<td>ITIL</td>
<td>Information Technology Infrastructure Library - Framework to manage IT infrastructure, development and operations</td>
</tr>
<tr>
<td>ITSA</td>
<td>Information Technology Security Advisor</td>
</tr>
<tr>
<td>ITSM</td>
<td>Information Technology Service Management</td>
</tr>
<tr>
<td>J6</td>
<td>Strategic Advisor (Strategic J6) to the Chief of Defence Force and Commander Joint Operations on communications and information systems and electromagnetic spectrum.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>The processes that maintain the current state of ICT Infrastructure represented by the existing baseline</td>
</tr>
<tr>
<td>MOTS</td>
<td>Military off the Shelf</td>
</tr>
<tr>
<td>MSPC</td>
<td>Military Sub-Portfolio Committee - Committee specific to the Military stakeholder group</td>
</tr>
<tr>
<td>NPOC</td>
<td>Net Personnel and Operating Costs - Defined by the net impact a capability will have on operating costs (i.e. what it will cost to sustain the capability)</td>
</tr>
<tr>
<td>PABX</td>
<td>Private Automatic Branch Exchange</td>
</tr>
<tr>
<td>PMO</td>
<td>Portfolio Management Office</td>
</tr>
<tr>
<td>PRINCE2</td>
<td>Projects in Controlled Environments version 2 - a project management methodology currently utilised by CIO for delivery of ICT projects</td>
</tr>
<tr>
<td>PSP</td>
<td>Professional Service Providers</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switched Telephone Network</td>
</tr>
<tr>
<td>SET</td>
<td>Stakeholder Engagement Team</td>
</tr>
<tr>
<td>SG</td>
<td>Strategy Group</td>
</tr>
<tr>
<td>SOA</td>
<td>Services Oriented Architecture</td>
</tr>
<tr>
<td>SOCAUST</td>
<td>Special Operations Commander Australia</td>
</tr>
<tr>
<td>SPC</td>
<td>Sub-Portfolio Committee</td>
</tr>
<tr>
<td>Term/Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SRP</td>
<td>Strategic Reform Program</td>
</tr>
<tr>
<td>Sustainment</td>
<td>Sustainment is focused on maintaining the services and infrastructure that underpin the stakeholders consumption of service</td>
</tr>
<tr>
<td>UC</td>
<td>Unified Communications</td>
</tr>
<tr>
<td>VCDF</td>
<td>Vice Chief of the Defence Force</td>
</tr>
<tr>
<td>WofG</td>
<td>Whole-of-government</td>
</tr>
</tbody>
</table>