



Version 1.0, 30 June 2010  
OID: AB3819313  
DPS: JUN028-10

# Contents

Foreword	iii
Introduction	v
Overview	1
Purpose of a Charter	1
Relationship Management Channels	2
Initiatives to Improve Service Delivery	3
Strategic Imperative 1 - Optimise Defence ICT Investment	3
Strategic Imperative 2 - Closer Stakeholder Engagement and Alignment	4
Strategic Imperative 3 - Provide Agreed, Priority Solutions	5
Strategic Imperative 4 - Strengthen ICT Capability	6
To Request a New ICT Capability or Task	7
Commitment to Continuous Quality Improvement	7
Review and Feedback	7
How CIOG Determines When an ICT Request can be Closed	8
Expectations	9
What ICT Users can Expect from CIOG	9
Responsibilities of Defence ICT Users	9
Funding Principles	11
Annexes:	13
A. Baseline ICT Services	15
B. Additional ICT Services	19
C. Specialist ICT Services	23
Tables:	
A-1: Baseline ICT Services	15
B-1: Additional ICT Services	20
C-1: Specialist ICT Services	23

# Foreword

We are pleased to introduce this *Defence Information and Communications Technology (ICT) Services Delivery Charter* (the Charter) that describes the characteristics of the diverse ICT services provided to enable Defence personnel to do Defence business. These services are particularly critical to providing the Australian Defence Force with superior operations and intelligence capabilities, but are also extremely important for efficient and effective functioning of supporting administrative, logistics and other business processes. The Charter will be supplemented by an online ICT Services Catalogue with more detailed descriptions of the ICT services available to Defence personnel.

We consider this document to be a formal agreement between us on behalf of all Defence personnel as users of ICT services, and the Chief Information Officer (CIO) on behalf of all his CIO Group personnel, our ICT service providers.

We look forward to this Charter being a catalyst for continuing to improve dialogue between all Groups and Services on how ICT services are delivered and supported across Defence, and how we all make best use of ICT resources and information superiority to defend Australia and its interests. We expect that such dialogue will always include the CIO Group whenever a service or requirement involves the flow of data into, through or from the Defence Information Environment, or uses its limited resources such as user devices and electromagnetic spectrum.



**Dr I. J. Watt, AO**  
Secretary



**A.G. Houston, AC, AFC**  
Air Chief Marshal  
Chief of the Defence Force



# Introduction

This *Defence ICT Services Delivery Charter* is intended to assist you, the users of ICT, to access ICT services and to help my CIOG staff to provide you with ICT services that are continuously being monitored, measured and improved to better meet your business and operational requirements. To assist you in formulating your requirements, expectations and priorities we have established three Stakeholder Engagement Teams (SETs) based on the Military, Corporate and Intelligence domains. The SETs will be further developed to provide you, in conjunction with our Customer Engagement staff, with a more consistent 'front door' to CIOG for specific domain services. The Defence Information Infrastructure common to all three SETs will be handled as a separate portfolio of activity by the CIOG Chief Technology Officer.

The Charter sets the standards of service that you can expect from CIOG, provides information about contacting us to seek information/assistance or to provide feedback, and describes both our commitment to you and our expectations of you. It applies to everyone who supplies and uses our services, or who seeks information from us about efficient and effective management and delivery of information in support of Defence business and operations.

I encourage you to use this Charter as a reference tool in your dealings with the CIOG. The commitments made in this document apply across all our ICT business and operational services as listed in the Defence ICT Services Catalogue available on the CIOG website.

I authorise the use of this Charter and commit, on behalf of all CIOG personnel, that, within the limitations of my Directive and allocated resources, the details herein will be used to guide our 'best effort' endeavours to meet or surpass the service levels. This will require the continued support and assistance of the ICT service providers in the other Groups and Services.

I am committed to the continuous improvement of our service delivery and welcome your comments and feedback.



**Mr Greg Farr**  
Chief Information Officer



# Overview

## Purpose of a Charter

1. **Defence Strategic Reform.** As part of the [2009 Defence White Paper](#) and the Information and Communications Technologies (ICT) Strategy 2009 suite of reforms, Defence will implement a new, outputs-driven budget management model that gives capability managers, in close consultation with all Group Heads and Service Chiefs, greater control of the total cost of delivering their capability outputs. There will be greater visibility of the true costs of goods and services used within Defence, without the need for complex transfer pricing arrangements. This model, which will drive support cost savings for reinvestment, is based on clear, precise and documented service level agreements and other performance management arrangements. This Defence ICT Services Delivery Charter (the Charter) records these agreements to guide the more detailed guidance in the *Defence ICT Services Catalogue* (the Catalogue). The Catalogue is the online tool for users to gain current knowledge about an ICT service; particularly how to request it and the quality performance they can expect.
2. **An ICT service** can be considered any assistance/support available or provided to enable any person to more efficiently use ICT, eg access to and technical support for computer networks, software applications and communications devices. ICT services include any request for change (move, additional capability or improved quality performance). They can be either dedicated to a sole/single user with a workstation/office or shared among common/multiple users in a barracks environment.
3. **Defence users** are only to obtain these services from CIOG, or the Intelligence and Security Group and Defence Science and Technology Organisation (DSTO) ICT, where indicated in the annexes. In the case of applications or commercial software the Chief Technology Officer (CTO) Division is to be contacted, via the relevant Stakeholder Engagement Teams (SETs): Military SET (MILSET), Corporate SET (CORPSET) and Intelligence SET (INTSET) to arrange product selection and/or purchase. The Defence Materiel Organisation (DMO) and I&S Gp retain some delegated authority for software, working with CTO Division.
4. **Types of ICT service.** This Charter is a dynamic document that will reflect shifting demand priorities on Defence ICT. Annexes A to C provide the general detail on the basis of provisioning, funding arrangement and some performance metrics for the following types of ICT service:
  - a. **Baseline** ICT services are available to all Defence personnel who have a justified business need/ operational requirement and the relevant level of security clearance. These services are requested via the relevant Service Desk or self-service tool and are generally funded centrally by CIOG. Examples are access to a secured and non-secured fixed telephone, audio/video conferencing and fax, and accounts to access the Internet, Defence Restricted, Secret and Top Secret Networks (DRN, DSN and DTSN) as required. For some users, access may be limited to a shared terminal or facility available in the local area, rather than to a dedicated resource.
  - b. **Additional** ICT services are provided to individual ICT account holders in addition to the baseline services, on request to the relevant Service Desk. Although bulk equipment purchases, enterprise

licences and mobile ICT devices for senior officers/executives will be funded centrally by CIOG, user Groups will usually be required to provide funding, based on the funding principles provided in paragraph 30. Examples are mobile ICT services or terminals dedicated or tailored to the user's needs, but using items from the Defence standard hardware or software lists.

- c. **Specialist** ICT services are specific to a certain group of users or community of interest. To facilitate more consistent agreements with the relevant stakeholders, specialist ICT services in Defence have been aligned with the Military, Corporate and Intelligence business domains. The MILSET, CORPSET and INTSET negotiate with user representatives of their business domain to ensure services meet their unique, often time-limited requirements. Funding is generally provided by the requesting Group. Examples are services in support of a specific military operation or access to intelligence systems for specific intelligence analysis users.
5. **A single agreement.** This Charter aims to minimise the need for multiple service level, operational performance, workforce and other agreements between CIOG and all Groups, Services, stakeholders and communities of interests. When requirements need to be specified for a particular system or functional area, the agreements between CIOG and the relevant business area will be incorporated into an annex of this Charter. These annexes include broad performance requirements on aspects such as a system's availability, but the Catalogue will provide more detailed metrics and relevant contact details for each service. When automated data collection and analysis tools are available, both the Charter and its supporting Catalogue will provide better service standards against which the CIO and the CIOG can be held to account.
  6. **ICT service delivery partners.** The Charter does not distinguish between services that CIOG provide directly and those delivered by other service delivery partners. The DMO has established materiel acquisition, sustainment and shared services agreements and (MAAs, MSAs and SSAs) with CIOG and other Defence Groups, but other service delivery partners that contribute to the provision of Defence ICT include:
    - a. the Defence Support Group (DSG), eg Office Machines Section for multifunctional devices and the resupply of consumables;
    - b. Tactical Information Integration Office (TIEIO) and Command and Intelligence Systems Support Office (CISSO) in the DMO;
    - c. Industry partners; and
    - d. the Services, with ICT specialists in most units, but particularly the Royal Australian Corps of Signals, Communications Centres, No 1 Combat Communication Squadron, and the Fleet Information Systems Support Organisation (FISSO).

## Relationship Management Channels

7. In addition to this Charter and the Catalogue, there are other relationship management channels covering CIOG services. These include any committee, working/management group or other forum where concerns on CIOG services can be raised. In conjunction with establishing the SETs, CIOG is also

working with Services and Groups to support their role in deciding priorities for their ICT requirements, through their respective Group's ICT Point of Contact (GPOC) and the relevant ICT Sub-portfolio Committee (SPC), ie Military, Intelligence or Corporate. If necessary, issues can be further escalated through these forums to the Defence ICT Committee (DICTC) and the Defence Committee (DC).

8. **Business Process Owners (BPOs).** Applications, particularly corporate applications such as ROMAN, PMKeyS and SDSS are delivered in conjunction with their respective BPO. CIOG does provide infrastructure and access to applications, but does not determine the business requirements and end-user support for all business applications. End user support for these applications is, at this stage, the responsibility of the relevant business area, eg the Chief Finance Officer Group for ROMAN.
9. **The Memorandum of Arrangement (MOA)** between Defence and DMO has introduced a system of MAAs, MSAs and SSAs. The CIO is the Lead Capability Manager for a number of the ICT capabilities, against which CIOG monitors and reports performance. The SSA between DMO and CIOG is available from the MOA website and as this Charter, the Catalogue and the SSA develop, their alignment will be improved.
10. **The Service Delivery Improvement Workshop** identifies opportunities for improvement in the delivery of ICT services and/or the user experiences and oversees the successful implementation of resolution initiatives. Participants include CIOG senior leaders and current contract vendors.

## Initiatives to Improve Service Delivery

11. This ICT Services Delivery Charter is a dynamic document. As Defence progressively implements the initiatives in the Defence ICT Strategy 2009, the nature and manner of ICT services delivery will continue to evolve and improve. As detailed in the Strategy, the following are the Implementing Strategic Imperatives and their enabling key initiatives that will impact ICT service delivery.

### Strategic Imperative 1 - Optimise Defence ICT Investment

12. Initiatives include the following:
  - a. **Consolidate Data Centres.**
  - b. **Reduce 'time-to-market'** ICT Two Pass process is an initiative that includes a new approvals framework for Defence-wide ICT investments, which is modelled on successful commercial practices and the whole-of-government process.
  - c. **Implement a Single Secure Desktop Program** to de-clutter the desktops of Defence personnel by introduction of multilevel information sharing across security domains.
  - d. **Develop Defence's Enterprise Architecting capabilities** to align Defence capabilities and outputs with Defence's strategic drivers, focussing on:

- (1) establishing the CTO Division with supporting governance over architecture and standards development;
  - (2) enhancing the current Defence Architecture Framework (DAF) to create the Integrated Defence Architecture (IDA);
  - (3) implementing the supporting strategic and technical control frameworks; and
  - (4) establishing and maintaining an integrated view of Defence's architectural direction for a common medium for communications between the business and ICT, while guiding strategic directions and planning.
- e. **Implement a Services Oriented Architecture (SOA)** to deliver the policies, processes, skills, tools and fundamental capabilities for the implementation of a multi-domain, Defence-wide SOA infrastructure that is based on the Defence Electronic-Business Infrastructure (DEBI) and Defence Online Services Domain (DOSD).
  - f. **Defence Information Environment (DIE) simulation and modelling** to help reduce costs and risks, but enhance ICT capability and architecture management. This will include close consultation with Joint Operations Command and the Services to ensure the deployed perspective is addressed from the start of such develop.
  - g. **Deliver distributed computing** in the Central Services Program to improve the management of those services that can be delivered remotely from a central location over the DRN, DSN and DTSN. This includes the Service Desks' services, the managing and monitoring of hardware, and the deployment of software updates.

## Strategic Imperative 2 - Closer Stakeholder Engagement and Alignment

13. Initiatives include the following:

- a. **New Stakeholder Engagement Model** will continue to develop the Intelligence, Military and Corporate SETs to improve interaction with the Services and Groups, with the shared infrastructure being handled as a separate portfolio of activity. CIOG, with assistance from its ICT service partners, will work with stakeholders to facilitate and improve their ability to prioritise ICT requirements via their respective ICT GPO and SPC. Each SET, in conjunction with their stakeholders, is responsible for:
  - (1) overall ICT service delivery to their stakeholders;
  - (2) providing a point of contact for Defence stakeholders for all ICT-related matters;
  - (3) understanding stakeholder requirements;
  - (4) ensuring stakeholders' business needs are represented within CIOG;

- (5) developing strategic ICT demand forecasts with stakeholders;
  - (6) assisting with development of proposals for new ICT capabilities with stakeholders; and
  - (7) informing broad ICT planning for the stakeholder group.
- b. **Improved sharing and access to services with key allies** aims to improve connectivity and information sharing through an Interoperability Improvement Program that supports the planning and conduct of combined operations and Defence business activities.
  - c. **Specialist business solutions design capability** 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.

### Strategic Imperative 3 - Provide Agreed, Priority Solutions

14. Initiatives include the following:

- a. **Information management (IM)**, including information assurance (IA), aims to provide a secure, competitive advantage in situational awareness, rapid decision making and the precise application of force over our adversaries. Effective and coordinated IM/IA 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 life cycle, which will be achieved by developing and implementing IM processes, policies, doctrine, skills, technologies and procedures Defence-wide.
- b. **Deliver unified communications (UC)** is an initiative that includes capabilities such as instant text messaging, voice calls, video calls, application sharing, presence and call recording using a common platform. The DSN UC Project will deliver the primary means by which some users of the DSN will electronically communicate via voice, and be capable of scaling to meet the needs of all DSN users.
- c. **Deliver a high-speed Defence Strategic Communications Network (DSCN)** includes Joint Project (JP) 2047 to improve the conduct of operations and the management of Defence business. It will deliver a high-speed DSCN that will include the wide area network and base area networks in Australia, links with selected fixed overseas sites, and interfaces to military communications and external partners.
- d. **Analysis of disruptive technology** initiative will use Defence 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.

## Strategic Imperative 4 - Strengthen ICT Capability

15. Initiatives include the following:

- a. **Sourcing strategy aims** to have more strategic relationships with fewer vendors to consolidate infrastructure sourcing into five bundles: distributed computing, centralised processing, terrestrial communications, specialist communications and applications.
- b. **Investing in people** initiative will include a Strategic Workforce Plan to provide broad direction at the whole-of-government level on how to improve the recruitment, retention and engagement of ICT personnel.
- c. **Information Technology Service Management (ITSM)** Program will implement ITSM as the discipline for managing ICT systems focused on the user's perspective of ICT's contribution to business. This includes the Defence ICT Services Catalogue, a corporate set of processes for interaction, incident, problem, change and release management based on Information Technology Infrastructure Library (ITIL) version 3 best practices, and a central DSN, DRN and Defence Voice Network (DVN) federated Configuration Management Database (CMDB) that supports change impact analysis across all ICT assets.
- d. **ICT Reform Portfolio Management** is the service review and evaluation as one part of ongoing business improvement activities, the implementation of ITIL v3 and the 10-year program of activities under the Defence Strategic Reform Program (SRP). The ICT Reform Portfolio Management Office (PMO) will coordinate, integrate and provide oversight of all reform activities.
- e. CIO, as **Coordinating Capability Manager** for all Defence ICT and the single DIE.
- f. **Infrastructure remediation** is a program of activity to replace aging desktops, printers, laptops, monitors, switchboards and other network equipment. It will include server, storage and backup remediation, and the replacement of all known out-of-warranty switch and router infrastructure.

16. **Enabling Defence Business Reform.** In addition to the initiatives 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.

17. **Defence Service Delivery Platform (DSDP).** Supporting the above ITSM initiative is the Service Desk Consolidation Project to collocate the existing DRN, DSN and DVN service desks using a Service Management suite of software tools based on Hewlett Packard Service Manager 7, Asset Manager and Decision Centre. Project Expedite will make available a new ICT Services Catalogue, an employee self-service portal, standard change requests and an end-to-end workflow automation of processes.

18. **Operations and business continuity improvements.** The Continuity of Defence Operations (CoDO)<sup>1</sup> remains a fundamental framework for the CIOG to manage disruptions to the delivery of critical ICT services to Defence. The five CoDO phases are: Preparation prior to an outage or emergency occurring, Immediate (within 2 hours), Interim (within 24 hours), Recovery (within 7 days)

<sup>1</sup> DI(G) OPS 45-1 - Policy and Procedures for the Continuity of Defence Operations

and Restoration (within 21 days). In the event that an outage extends beyond 21 days, alternative management arrangements will be established. The creation, implementation and testing of the CIOG's Business Continuity Plan (BCP) and disaster recovery (DR) procedures for critical functions is the responsibility of CIOG managers and commanders at all levels. The BCP includes business continuity and DR arrangements for each of the branches and/or business functions as annexes, identifies the Business Continuity Coordination Team (BCCT) composition, roles of the BCCT, and reporting requirements. For more detail contact the Directorate of Risk, Audit, Reporting and Evaluation (DRARE).

19. **Change Request improvements.** CIOG is refining how it handles smaller or incremental growth to the DIE. Often, a threshold needs to be defined, eg five terminals, up to which small growth can be handled as a job logged through the ICT Service Desk. Larger, above the threshold growth requires a business request and formal consideration, approval, prioritisation and separate funding by the requester's Group, eg using the funding principles detailed below.

### To Request a New ICT Capability or Task

20. The ICTBR process enables users to request changes to Defence's existing ICT capability. This includes requests for ICT consultancy services and the development and delivery of ICT projects in support of Defence's business needs. To seek new capability that is above the threshold for minor growth, the current approach is to raise an ICT Business Request (ICTBR) on Webform AD877, in accordance with the instructions on the form, and send it to ICT Business Requests. An electronic ICTBR portal is available to some Groups to facilitate this change process.
21. To lodge a new Project Proposal, complete the DIE Project Mandate Proposal. When an existing Project Mandate exceeds agreed resourcing or delivery milestones, or to change an existing Project Mandate, a Project Mandate Change Request (PMCR) is required.

### Commitment to Continuous Quality Improvement

22. Where the performance indicators are not met, CIOG is committed to undertaking a thorough analysis of the reasons for CIOG service delivery failure, and to rectifying the problems that this analysis uncovers. The performance thresholds set in this Charter are designed to improve service delivery quality incrementally, recognising that there is always room for improvement.
23. With each new release of this Charter, Defence will review performance indicators. This will be driven by competing priorities of the finite ICT resources.

### Review and Feedback

24. CIOG is committed to ensuring that this Charter reflects needs and expectations. To ensure CIOG can continue to improve the quality of ICT services, feedback is most welcome via the [Feedback link](#) from the [CIOG Home Page](#). Feedback may be either:

- a. a compliment about a particularly good service, if possible with the name of the person who provided it;
- b. a complaint about poor service, with a suggestion on how CIOG could possibly remedy the situation;
- c. a suggestion about how CIOG can improve the service to the user; or
- d. an enquiry about a service. The Directorate of Customer Engagement (DCE) will acknowledge the enquiry within four working days of receipt and coordinate the enquiry with the relevant area(s) for action/resolution.

DCE works in conjunction with the SETS to address individual through to Group level user feedback received, underpinned by ongoing user contact and consultation.

25. **Complaints.** When lodging a complaint about a service, it is important to be specific. If the complaint is related to a specific service request, eg if it was closed prematurely or was not courteously handled, then the user should contact the relevant Service Desk in the first instance and log another call stating that a complaint is being raised. For any other complaint, eg the user is not happy with the response received from the Service Desk in regards to a lodged complaint; provide details through the online [ICT Customer Feedback](#) form. A user with an issue about an ICT request being closed can also log their concern via this form or the link provided on the job-closure email.
26. **General enquiries.** For general enquiries, first browse the [CIOG website](#) for the information needed. It can be accessed from the DRN Home Page by selecting the 'Chief Information Office Group' link. The site includes:
- a. general information about CIOG;
  - b. a link to this Charter and the Catalogue;
  - c. online feedback forms;
  - d. specific information about the current status of the network, including scheduled and unscheduled interruptions to ICT services; and
  - e. information about key projects and other initiatives being undertaken within CIOG.

Users who are unable to find the information they need a specific service should let the relevant Content Manager know by using their address link on the bottom left of each webpage.

## How CIOG Determines When an ICT Request can be Closed

27. When a request has been closed by CIOG, the user will be advised by email. The following criteria is applied by CIOG when determining if a request should be closed:
- a. The request has been resolved or a workaround has been applied.

- b. It has been accepted for action by a Service Desk external to CIOG or another Defence contact.
- c. It has been accepted by a regional site administrator as a local application or terminal configuration issue.
- d. CIOG has been unable to make contact with the person who made the request after three unsuccessful attempts (via telephone and email) over three working days.

## Expectations

### What ICT Users can Expect from CIOG

28. **CIOG's commitments.** CIOG aims to provide users with a high quality service, in accordance with this Charter and the Catalogue. CIOG personnel will:
- a. assist the ICT user and be responsive to their needs;
  - b. actively keep the user informed of the progress of their request for service or support;
  - c. provide the user with timely oral and written advice that is clear, concise, accurate and complete; and
  - d. consult with the user and other stakeholders regarding issues that will affect them.
29. **CIOG's behaviour.** In providing services to users, CIOG personnel will:
- a. adhere to the Defence and/or Public Service values;
  - b. accept initial ownership of the issue that led the user to contact CIOG, although CIOG may pass the request to another, more relevant area for resolution;
  - c. be courteous;
  - d. treat users fairly and professionally; and
  - e. help users to escalate issues as required, eg through the relevant SET.

### Responsibilities of Defence ICT Users

30. **ICT users' responsibilities.** To help CIOG provide acceptable services, ICT users are to:
- a. adhere to the Defence and/or Public Service values;

- b. comply with Defence's policy<sup>2</sup> on the proper, appropriate and reasonable use of Defence telephone and computer resources, eg that users:
  - (1) do not undertake actions which might damage the network or Defence's reputation;
  - (2) do not use it for illegal purposes;
  - (3) do not abuse the policy of reasonable personal use of some Defence ICT resources during normal working hours; and
  - (4) do not attempt to locally modify approved network specifications, architectures or settings;
- c. understand the ICT service delivery commitments that CIOG has made in this Charter and the Catalogue;
- d. access Service Desks responsibly, eg before calling the Service Desk:
  - (1) check any Frequently Asked Questions (FAQs) webpage and other self-service options; and
  - (2) if calling about a problem with hardware or software, try to reproduce the problem so that the Service Desk staff will have an accurate sequence of events to assist them with the diagnosis;
- e. understand that not all calls to the Service Desk have the same priority, eg operational issues and large scale outages take precedence over issues affecting only one user;
- f. improve their knowledge about the single DIE and their personal skills to safely and efficiently use network tools, eg by doing training courses and online tutorials on the software applications that they may need;
- g. provide accurate contact details when a service is requested, and check for email and voicemail regularly to see if there is an action required to progress the request;
- h. provide constructive feedback, complaints, compliments and suggestions on ways to improve CIOG services to the ICT service users; and
- i. provide timely advice to CIOG of any changes to the user's requirements or circumstances that may affect the work requested.

<sup>2</sup> Particularly DI(G) ADMIN 10-6 - *Use of Defence Telephone and Computer Resources*

# Funding Principles

31. CIOG personnel apply the following principles when determining if CIOG or the user's Group will provide the necessary funding for Defence ICT services:

a. **Principle 1. CIOG will not charge for basic or necessary ICT services that have been approved for the DIE.** These include the following:

- (1) Desktop or laptop computer for CIOG controlled networks.
- (2) Network infrastructure devices.
- (3) Desktop phone.
- (4) Mobile phone.
- (5) BlackBerry devices for Category A and B users, as defined in annex B.
- (6) Secure Mobile Environment - Personal Electronic Device (SME-PED), except to other government agencies.
- (7) Leased lines to a Defence base/site/barracks.
- (8) Storage/Computing in a CIOG-managed data centre, except for non-Defence applications supported by CIOG on a cost-recovery basis.
- (9) Microsoft (MS) Office suite.
- (10) DRMS/EDMS applications.
- (11) Moves, adds and changes for small changes to the DIE.

b. **Principle 2. User charging is used to provide cost transparency and support cost consciousness.** Items that are charged to the user Group are in essence discretionary items of ICT expenditure, and include the following:

- (1) Wireless network cards.
- (2) BlackBerry devices for Category C users, as defined in annex B.
- (3) Non-standard software applications, eg MS Project and Visio.
- (4) Major building moves.
- (5) Overseas offices.

(6) Specialist ICT needs where the capability already exists elsewhere in the DIE.

- c. **Principle 3. CIOG will attempt to negotiate and source enterprise licence agreements (ELAs) and software licence rationalisation with all major software suppliers to Defence.**  
This should either remove any need to charge, or reduce the amount of the charge to a user's Group for the service.
- d. **Principle 4. The cost and access to ICT services, including products, from CIOG will be promoted via the Catalogue** as the only source of ICT services for Groups outside of direct engagement with the SETs.
- e. **Principle 5. The user charging will be levied at Group level, not at individual level** to minimise costs of administration on an annualised basis, unless it is for cost recovery due to negligent damage or misuse of ICT devices or services.

# Annexes

- Annex A - Baseline ICT Services
- Annex B - Additional ICT Services
- Annex C - Specialist ICT Services







## A-4: Baseline ICT Services cont.

Ser	Service Element	Ability and Service Objective
10	Shared access to Defence audio and video teleconference (VTC) services	Shared user access to audio or videoconferencing facilities or the Defence Secure Videoconferencing Environment (DSVE) is dependent on demand within each region, and can only be provided as best effort support. DSVE enables combined real-time audio and visual communications to support Defence operations and business functions. Secure conferences can be booked via the DSVE Videoconference Network Operations Centre (VNOC) and are funded by CIOG. UNCLASSIFIED services are funded by the user's Group, in consultation with the CIOG.
11	Support to the above services	Support services include technical support via the national and regional service desks, training (initial and update) tools, documentation access and development, equipment fleet configuration and records management, application and licence management.
12	Access to the DRN's Document and Records Management System (DRMS) and/or DSN's Electronic Document Management System (EDMS)	The DRN preferred application for filing and archiving of defence records. The DSN preferred application for filing and archiving of Defence records. Support requests will be passed to the Applications's Service Desk or Business owner (Directorate of DRMS).

<sup>3</sup> A 'day' or 'hour' is a normal working day or hour from logging a job with the relevant Service Desk.

## Additional ICT Services

1. **Additional ICT services**, as listed in Table B-1, are provided to Defence individuals with an ICT account and a justified business requirement. They are in addition to the baseline ICT services but also requested via the relevant Service Desk. Further details are in the Defence ICT Services Catalogue. Although bulk equipment purchases, enterprise licences and mobile ICT devices for senior officers/executives will be funded centrally by CIOG, user Groups will usually be required to provide funding.
2. **Categories of users.** For certain mobile ICT devices and services detailed in Table B-1, users have been categorised to allow CIOG and GPOCs to prioritise the basis of provisioning of limited resources. The three categories of users defined by the Defence ICT Committee (DICTC)<sup>4</sup> are as follows:
  - a. **Category A.** Very Important Persons (VIPs), as defined by the Continuity of Government Agreement (CODA), Senior Leadership Group (SLG) members and their primary Military Assistant, Executive Officer or Military/Defence Attaché<sup>5</sup>.
  - b. **Category B.** Military commanders at the Officer-5/6 rank levels appointed by a formal instrument of command.
  - c. **Category C.** Other staff as authorised by a financial delegate and GPOC in the user's Group.
3. **Levels of user service.** To improve service responsiveness, quality and support to the more important of our users, CIOG has developed a VIP/SLG Support Model for service requests by Category A users. The following, more significant elements of the model allow CIOG to scale services based on known requirements:
  - a. **VIP/SLG 24/7 Service Desk.** Priority user hotlines operates 24 hours every day (24/7) to increase the VIP/SLG first level resolution rates and provide a more personalised user experience. Special telephone numbers are provided for use as the first point of contact for this service.
  - b. **VIP/SLG 24/7 escalation contact.** These ICT users have a dedicated contact in the Directorate of Customer Engagement (DCE) for escalating urgent or overdue ICT service requests. DCE will ensure ICT services delivery to VIP/SLG users is responsive, timely, and coordinated. DCE VIP Support provides more dedicated support specifically to the Minister/PARLSEC/SEC/CDF users.

<sup>4</sup> DICTC meeting Minutes of 30 Nov 09.

<sup>5</sup> Military Attaché is an official under the authority of an Ambassador or other head of diplomatic mission, who serves either as a diplomat or as a member of the support staff.

- c. **VIP on-site support.** A specialised and trusted on-site response team with a high level of technical responsiveness and an awareness of sensitivities when servicing VIP users is available between DCE and the individual using the service.
- d. **Improved CIOG user service protocols.** This allows better problem identification, prioritisation method, problem resolution and project support.
- e. **Positive hand-off of VIP tasks.** Tasks transferred from the VIP Service Desk to Defence Service Delivery Lines will include positive hand-off (phone call or visit) to alert the delivery areas of the importance of the task.

Table B-1: Additional ICT Services

Ser	Service Element	Ability and Service Objective
1	Non-standard desktop, fixed telephone or ancillary for the Defence Voice Network (DVN)	This could include assistive technology for OHS or users with a disability, a press to talk telephone or cordless telephone, a telephone credit card, data modem connection to the PSTN, etc.
2	Mobile telephone and account	Issued on approval of a Band 1/1 Star or above, but not in addition to a BlackBerry device. Funded by CIOG, but if use is assessed as not compliant with Defence policy <sup>6</sup> , reimbursement may be required. Telephone accounts that have not been used for over three months will be considered for termination if not justified.
3	BlackBerry device and account	Issued in accordance with the following categorisation: * Categories A and B. Funded by CIOG. * Category C. The cost for the device and ongoing usage are charged to the ordering Group. If use is assessed as not compliant with Defence policy <sup>6</sup> , reimbursement may be required.
4	Secure Mobile Environment - Personal Electronic Device (SME-PED)	The SME-PED Project has introduced an interim capability with a limited number of USA DoD devices. A roll-out of a DSN capable SME-PED is expected to be undertaken in 2011. This capability would be CIOG funded except for devices provided to other government agencies.
5	Voice Over Internet Protocol (VOIP) and Unified Communications (UC)	DSN VOIP and/or UC access, terminals and support will be considered on a case-by-case basis, funded by the requesting user's Group.
6	Non-standard desktop computer terminal and/or ancillary for DRN/DSN/DTSN	If approved, funded by the requesting user's Group.

<sup>6</sup> Including [DI\(G\) CIS 6-7-002 - Mobile Telephones and Related Services](#) and [DI\(G\) ADMIN 10-6 - Use of Defence Telephone and Computer Resources](#).

## B-2: Additional ICT Services cont.

Ser	Service Element	Ability and Service Objective
7	Non-standard or additional DRN/ DSN/DTSN printer or scanner	If approved and the printer/scanner falls inside the standard coverage for the required work area it may be funded by CIOG, otherwise by the requesting delegate, but in conjunction with DSG for multifunctional device (MFD) support and all consumables.
8	Additional software application licence and access on the DRN/ DSN/DTSN	CIOG will enable access to acquire and/or support required software application licences as detailed in the <a href="#">CIOG Instruction (CIOGI) 6/2007 - Applications Management and the Defence Approved Software List (DASL)</a> . User-specific applications that have been approved for use on CIOG controlled networks may require funding from the user's Group for additional licences. Unapproved applications that have not yet been assessed by CIOG, are deemed obsolete, or have been rejected as unsuitable must not be installed on CIOG controlled networks.
9	Laptop computer and ancillaries	Defence laptops (UNCLASSIFIED to SECRET) will be imaged with SOE application suite. This includes support for the Laptop Encryption Registration Application (LERA). Funded by CIOG if standard purchased centrally or by requesting delegate if non-standard.
10	Wireless data-card	Issued on Band 1/1 Star or above delegate's approval, as cost for use is charged to the ordering Group.
11	Defence Remote Electronic Access and Mobility Service (DREAMS) token and access	Enables a user to remotely connect to the DRN while away from the normal work location, eg travelling throughout Australia or at home after normal work hours. The SETs determine allocation of tokens to Category C users in consultation with GPOCs. All categories funded by CIOG. The mode and method of access are the responsibility of the user's Group. For a token transfer, advise the DRN Service Desk the token number, current incumbent, and the new incumbent's DRN username.
12	Home computing equipment for SLG members	In accordance with the Senior Executive Service Australian Workforce Agreement (AWA) and the Star Rank Remuneration Arrangement (SRRS) entitlements.

## B-3: Additional ICT Services cont.

Ser	Service Element	Ability and Service Objective
13	Electromagnetic spectrum (EMS) support	<p>The CIOG, through the Defence Spectrum Office (DSO) as the Defence Authority for allocation of EMS, will:</p> <ul style="list-style-type: none"> <li>- acquire and hold all licences on behalf of Defence for all RF emitters and receivers;</li> <li>- ensure compliance with, and provides advice on, the national and international regulatory requirements under the Radiocommunications Act and International Telecommunication Union Radio Regulations;</li> <li>- investigate for rapid rectification of all Defence RF interference occurrences;</li> <li>- maintain the Defence Strategic Spectrum Plan for all current and future Defence capability acquisition;</li> <li>- advise on technical policy and planning of radiofrequency (RF) availability and interoperability for all Defence platforms and equipment;</li> <li>- coordinate international and all Defence satellite assets; and</li> <li>- advice on the RF protection of satellite ground stations.</li> </ul>
14	Russell Video Network (RUSVIDNET)	RUSVIDNET terminals are available in common areas and some executive offices throughout Canberra, with support as detailed in the Defence ICT Services Catalogue on the DRN. To request a terminal contact the Voice Service Desk and change process. New connections incur the first year's Foxtel (if required) licence costs payable by the user's Group.
15	Thumb drive for classified data storage	A USB port thumb drive is being assessed for secure use on the DRN. If accredited, it must be used in accordance with security policy. Funded by the user's Group.
16	Support to the above services	Support services include technical support via the relevant national and regional service desks, training (initial and update) tools, documentation access and development, equipment fleet configuration and records management, and the approved software list records and licence management.

## Specialist ICT Services

1. **Specialist ICT services** detailed in Table C-1 are specific to a certain Defence group of users or community of interest through the relevant Stakeholder Engagement Team (SET). To facilitate more consistent agreements with the relevant stakeholders, specialist ICT services in Defence have been aligned with the Military, Corporate and Intelligence business domains. The Military SET (MILSET), Corporate SET (CORPSET) and Intelligence SET (INTSET) negotiate with user representatives of their business domain to ensure services meet their unique, often time-limited requirements. Funding is generally provided by the requesting user's Group.

Table C-1: Specialist ICT Services

Ser	Service Element	Ability and Service Objective
1	New or upgrade to Enterprise Resource Planning (ERP) software application acquisition, licence and support	<p>Specialist access to ERP applications, such as PMKeyS, ROMAN and SDSS will be negotiated with the CORPSET for availability of 24 hours every day (24/7), except during overnight batching and quarterly maintenance, which will be conducted in low demand periods. For PMKeyS, see DSG's <a href="#">System Availability website</a>. In the event of an outage, services will be restored in accordance with the CIOG Business Continuity Plan (See paragraph 18).</p> <p>Funding includes net personnel and operating costs (NPOC) through-life support arrangements detailed in annex G to the CIOGI 6/2007. Funding for a new application or application upgrade will be determined on a case-by-case basis by CIOG and the enterprise process owner.</p>
2	New or upgraded operational software application acquisition, licence and support	<p>Specialist access to operational applications, such as command and control, intelligence and situational awareness will be negotiated with the MILSET and/or INTSET for availability of 24/7, except during overnight batching and quarterly maintenance, which will be conducted in agreed low demand periods. In the event of an outage, services will be restored in accordance with the CIOG Business Continuity Plan (See paragraph 17).</p> <p>Funding includes NPOC through-life support arrangements detailed in annex G to the CIOGI 6/2007. Funding for a new application or application upgrade will be determined on a case-by-case basis by CIOG and the enterprise process owner.</p>

## C-2: Specialist ICT Services cont.

Ser	Service Element	Ability and Service Objective
3	Military formal messaging	Available 100% of time during the servicing communications facility's promulgated operating hours, with skilled personnel to transmit, deliver or notify the addressee within: <ul style="list-style-type: none"> <li>- <b>Three hours</b> for IMMEDIATE</li> <li>- <b>Six hours</b> for PRIORITY</li> <li>- <b>24 hours</b> for ROUTINE.</li> </ul>
4	Mobile ICT devices to specialist groups above the allocation as additional ICT services: <ul style="list-style-type: none"> <li>- Laptop computer and ancillaries</li> <li>- Non-standard mobile telephone or ancillaries</li> <li>- BlackBerry to Cat C users</li> <li>- DREAMS to Cat C users</li> <li>- SME-PED to Cat A, B and C users</li> <li>- Accredited USB devices</li> </ul>	Funded by the user's Group, subject to availability and SET negotiated priority/basis of provisioning. TOP SECRET and above Defence laptops will be funded by Intelligence and Security Group (I&S Gp) if they are from the standard hardware list purchased centrally or otherwise by the requesting unit. It will be imaged with SOE application suite and support for the accredited encryption application.
5	Access and support to non-SOE/non-DASL hardware/software applications, eg Linux and collaboration tools	Availability as negotiated with the relevant SET, application architectures and security accreditation personnel in CIOG.

## C-3: Specialist ICT Services cont.

Ser	Service Element	Ability and Service Objective
6	<p>Military networks and/or systems access, including:</p> <ul style="list-style-type: none"> <li>- CENTRIXS International Security Assistance Force (ISAF) as part of the Afghan Mission Network (AMN) enclave</li> <li>- CENTRIXS Four Eyes (CFE)</li> <li>- Secure Internet Protocol Router Network (SIPRNET) Releasable to Allies (REL-A) Access</li> <li>- Global Counterterrorism Force (GCTF) Information System</li> <li>- USA CENTCOM Naval Forces Component (CNFC)</li> <li>- The ADF Requirements Development Information System (TARDIS)</li> <li>- Air Component - Command and Control Weapon System (AC-C2WS)</li> <li>- Battlefield Information Collection and Exploitation Systems (BICES)</li> <li>- Coalition Maritime Forces Pacific (CMFP)</li> <li>- Joint Cross Domain Exchange (JCDX)</li> <li>- Tactical Environmental Support System (TESS)</li> <li>- Special Operations Command Support System (SOCSS)</li> <li>- Joint Training and Experimentation Network (JTEN)</li> <li>- Cadet Net</li> <li>- Radio Over Internet Protocol (ROIP)</li> <li>- High frequency (HF) communications</li> <li>- Very low frequency (VLF) communications</li> <li>- Amenities Internet</li> </ul>	<p>Provided jointly by CIOG as negotiated with the MILSET, FISSO and CISSO to deployed forces, HQ and the support echelon in direct support of MEAO operations. Interfaces to the strategic networks supported by CIOG. Levels 1-3 support is via the CIOG's Service Desk.</p> <p>SIPRNET REL-A provided via CIOG to authorised Defence users. Levels 1-3 support by CIOG and USA Defense Information Systems Agency (DISA). Used in accordance with security policy and procedures. Application details are on the DSN at \\DSN Home page\Joint Sites\Coalition IE.</p> <p>GCTF Information System is the bearer for the SECRET virtual private network for the CNFC. GCTF access and level 1-3 support provided via CIOG. CNFC supported by FISSO.</p> <p>TARDIS DRN instance supported by DMO via a service desk (working day only). DSN instance supported by CIOG via a service desk (working day only).</p> <p>For BICES, levels 1-3 support by the NATO BICES Agency (NBA).</p> <p>JTEN is a GBR/USA system provided to HQJOC approved users.</p> <p>HF communications are high availability system under control of CIOG Defence Network Support Agency. Infrastructure is provided and supported by a DMO Service Delivery contract.</p> <p>VLF communications is a 24/7 capability in support of operations of RAN and allied ships and submarines. It is provided through a DMO Service Delivery contract from the Harold E. Holt facility at Exmouth.</p> <p>Amenities Internet access provided in accordance with logistics policy and the communications annex of the relevant operations order.</p>

## C-4: Specialist ICT Services cont.

Ser	Service Element	Ability and Service Objective
7	<p>Intelligence networks and/or systems access, including:</p> <ul style="list-style-type: none"> <li>- Australian Special Communications Network (ASCON)</li> <li>- Joint Intelligence Support System (JISS)</li> <li>- Defence Imagery and Geospatial Organisation (DIGO) Net - Strategic Imagery Receipt and Exploitation Node (SIREN)</li> <li>- Defence Intelligence Organisation (DIO) Net</li> <li>- Defence Signals Directorate (DSD) Net</li> <li>- Integrated Broadcast Service - Intelligence (IBS-I)</li> <li>- Dissemination Information Services Geospatial Imagery Secret Environment (DISGISE)</li> <li>- STONEGHOST</li> </ul>	<p>ASCON provides secure and timely transfer of Signals Intelligence (SIGINT), electronic warfare (EW) data and other information to and from operational and tactical level operations centres and EW assets, DIO and DSD.</p> <p>All supported by I&amp;S Gp for 99.96% availability. CIOG support is via the INTSET.</p>
8	<p>Corporate networks and/or systems access, including:</p> <ul style="list-style-type: none"> <li>- Ministerial Communications Network (MCN)</li> <li>- DMO services in accordance with the DMO's Shared Services Agreement (SSA)</li> <li>- Assistive technologies to disabled users</li> <li>- Combined Federated Battle Laboratory Network (CFBLNET)</li> <li>- Defence Science and Technology Organisation (DSTO) RESTRICTED and SECRET networks</li> </ul>	<p>CFBLNET provided by CIOG as negotiated with CORPSET to Defence in support of multinational research, development, test and evaluation (RDT&amp;E) activities. Levels 1-3 support provided by CIOG.</p> <p>Supported by DSTO for 99.96% availability.</p>

## C-5: Specialist ICT Services cont.

Ser	Service Element	Ability and Service Objective
9	Satellite Communications (SATCOM): <ul style="list-style-type: none"> <li>- Military wideband: X and Ka-band</li> <li>- Commercial wideband: Ku and C-band</li> <li>- Military narrowband: UHF SATCOM</li> <li>- Commercial narrowband:               <ul style="list-style-type: none"> <li>• Inmarsat</li> <li>• Iridium</li> <li>• Defence Mobile Communications Network (DMCN)</li> </ul> </li> <li>- Blue Force Tracker (BFT) Off-platform service</li> </ul>	<p>CIOG maintains 24/7 global coverage (except polar regions) to military wideband and UHF SATCOM services, and 24/7 service desk services through the Defence Network Operations Centre (DNOC) in accordance with ADF Communications Instruction (ADFCI) 6.5.1.</p> <p>CIOG obtains access to commercial wideband services when Groups are unable to use military wideband services. Funding of commercial wideband is through operational funding.</p> <p>Inmarsat terminals provided by DMO and CIOG provides 24/7 global coverage to approved users.</p> <p>Groups acquire Iridium satellite phones through DMO. CIOG provides global 24/7 coverage to approved users for both secure and non-secure Iridium phones.</p> <p>DMO provides the DMCN service for the Australian region only. CIOG provides 24/7 service desk support services.</p> <p>BFT equipment is provided by DMO. CIOG provides 24/7 coverage for the Australian region only.</p>
10	Multinational Information Sharing (MNIS) Gateway	Provided by CIOG and includes AUS-USA, AUS-GBR, AUS-4Eyes, AUS-CFE, AUS-5Eyes and AUS-NZL. Levels 1-3 support provided by CIOG
11	Theatre Battle Management Core Systems (TBMCS)	Provided to RAAF by a DMO service delivery contract. CIOG provides high availability bearers for the system.
12	Support to the above services	Support services include technical support via the relevant national and regional service desks, training (initial and update) tools, documentation access and development, equipment fleet configuration and records management, and the approved software list records and licence management.



**Australian Government**  
**Department of Defence**