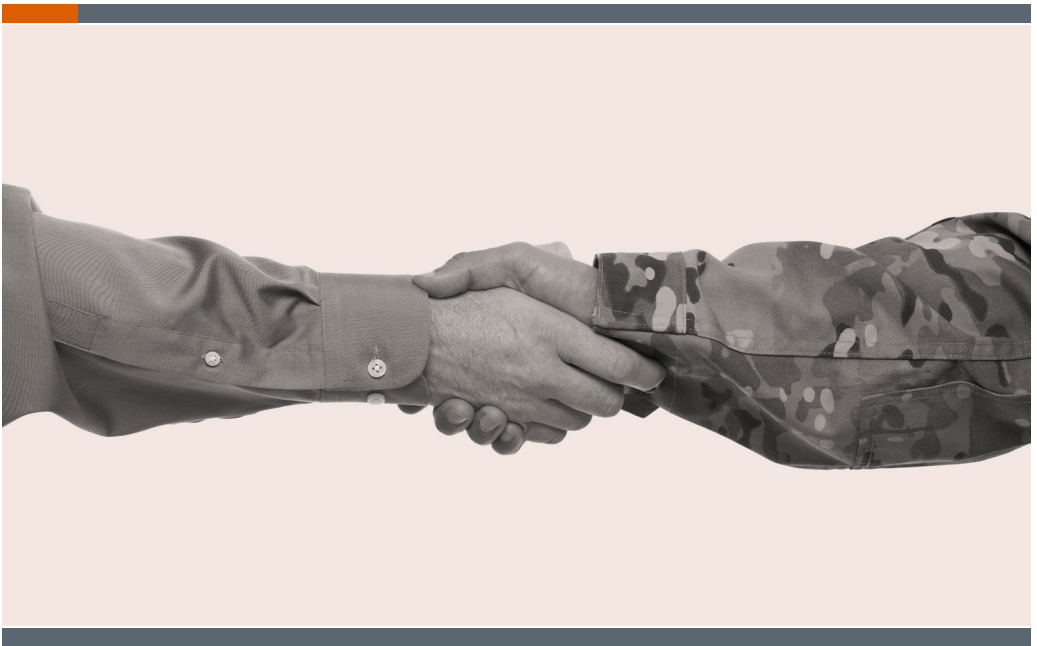




Australian Government
Department of Defence

DOING BUSINESS WITH CIOG — OPPORTUNITIES FOR INDUSTRY

Chief Information Officer Group (CIOG)



Our mission

The Chief Information Officer Group (CIOG) within the Department of Defence leads the integrated design, cost-effective delivery and sustained operation of Defence's Single Information Environment (SIE) to support military and business operations.

In simple terms, the SIE encompasses the information, computing and communications infrastructure of the Department of Defence along with the management systems and people that deliver that infrastructure.

It includes Defence's information assets, computing networks, business applications and the data that they generate and carry. It includes the communication standards and spectrum required for Battlespace networks. The infrastructure CIOG provides is essential and integral to core Defence functions including intelligence, surveillance, reconnaissance, communications, information warfare, command and management.

It is the responsibility of CIOG to ensure Defence has a dependable, secure and integrated information environment, capable of supporting its operational and management needs. We do this through delivering information, infrastructure and services.





Defence's SIE facts

CIOG:

- manages one of the largest information and communications technology (ICT) networks in Australia
- conducts business of around \$1.3 billion in support of Defence operations around the world
- manages and maintains over 134 000 workstations, 8400 servers, 3000 applications, has arrangements to access four defence-owned satellite payloads, as well as maintaining shared access to other allied satellites and three primary data centres for around 133 000 users
- manages Defence's fixed and mobile networks around Australia and internationally.

Our operating model

The **Chief Information Officer (CIO)**, who is the head of CIOG, is accountable to the Secretary for Defence and the Chief of the Defence Force (CDF) for the completeness and coherence of SIE planning; and for establishing effective governance and coordination arrangements for the development, operation and management of SIE capabilities. The authority of the CIO encompasses all aspects of SIE capability management including strategy, planning, prioritisation, development, implementation and support. The scope of that authority spans all Defence networks. The CIO is the technical authority for enterprise information management architecture, standards, policy and Master Data Management.

The **Chief Technology Officer Division (CTOD)** is responsible for the Defence ICT Strategy, technology road maps, architecture, and delivery of ICT systems and applications in line with Defence's goals and strategies. CTOD provides guidance and support to Defence on projects of strategic significance, promoting technology awareness and competence throughout the organisation. CTOD ensures applications are built and integrated in line with the architecture for applications and infrastructure, which is aligned with the SIE objective. Under new transformational changes, Business Relationship Management (BRM) has been integrated into CTOD. The role of the BRM is to manage CIOG partnerships with the Defence Groups and Services by anticipating, understanding and shaping their ICT and Information Management requirements to ensure that CIOG's efforts to enable and deliver Enterprise Information Management and ICT services are aligned with stakeholder priorities.

The **ICT Delivery Division (ICTDD)** is responsible for program and project delivery including development of capability acquisition proposals, and the design, development and implementation of capability solutions in the Defence SIE. ICTDD is also responsible for related industry engagement, consolidation and modernisation of Defence systems to improve service delivery to clients, and increase efficiency and effectiveness of business processes. Under new transformational changes underway across CIOG, the former **Infrastructure Transformation Program (ITP)** is being integrated into ICTDD. The ITP brings together key ICT transformation initiatives under a single program. The ITP addresses the requirement to manage dependencies, implement governance and synchronise delivery schedules across the five constituent projects: Terrestrial Communications, Centralised Processing and End User Computing, as well as IT Service Management Transformation and Stand Alone Networks Remediation.

The **ICT Operations Division (ICTOD)** (and Strategic J6) is responsible for the integration, operation, management and support of CIOG's components of the Defence SIE. It is also the Coordinating Capability Manager for key ICT capabilities including satellite communications, electromagnetic spectrum, high grade cryptographic systems, tactical data links, deployed networks and applications, and the Combined Federated Battle Lab Network.





Our projects

CIOG is undertaking a transformation program that will simplify, standardise and modernise Defence's ICT capability.

CIOG's key projects include:

- **End User Computing:** delivering the largest upgrade to the Defence Secret and Restricted networks in more than a decade. The upgrade includes Windows 2007+ and Office 2010, delivered largely through thin client architecture.
- **Terrestrial Communications:** upgrading more than 430 Defence sites to enable voice and video collaboration, Wi-Fi services, mobile device connectivity and advanced tactical interfaces.
- **Standalone Networks Remediation:** reducing security risk by establishing standalone network policy and decommissioning, accrediting, disposing, migrating or quarantining Secret and below networks.
- **Centralised Processing:** improving and simplifying Defence's ICT capability by consolidating Defence's computing infrastructure and applications from 280 data centres to 11 domestic and three international.
- **IT Service Management Transformation:** improving service management and service processes – reducing the number and impact of incidents and associated downtime.
- **Defence One:** delivering a sustainable, efficient human resources and payroll system for Defence with increased levels of automation, more accurate data, and improved self service options for end users.

Engaging industry

CIOG engages broadly with industry to develop and support ICT systems that provide capability and solutions to the Defence community, but more importantly, to support Defence operations. CIOG is transforming industry engagement from numerous contract-based interactions to fewer, deeper and more strategic partnerships.

As a service delivery organisation that works closely with a contracted workforce to deliver ICT support to Defence, it is important for CIOG to be responsive to the changing needs of its customer base.

To engage with CIOG, it is important that industry has an understanding of CIOG's accountability and compliance obligations in relation to:

- procurement policy, processes and practices including protocols for decision making and contract management
- tendering and contracting templates (including statement of work and quotations under standing-offer panel arrangements)
- documentation requirements and disclosure obligations
- protocols for procurement complaints handling, stakeholder consultation and management
- protocols for security and safety management
- ethics, probity, and risk management.

CIOG must ensure 'proper use' of Commonwealth resources and achieve value for money outcomes within the Commonwealth's resource management framework and procurement policy framework. CIOG seeks to ensure procurement processes are commensurate with the scale, scope and risk of the business requirement

CIOG acknowledges that industry needs to know the Group's strategic priorities and forthcoming opportunities. To meet this requirement, CIOG publishes its open approaches to market on the AusTender website at www.tenders.gov.au. CIOG may also use other appropriate channels to inform and engage industry on ICT initiatives.

To further expose products and capabilities across Defence, defence industry can access established channels such as the Unsolicited Innovative Proposals (UIP) and Unsolicited Promotional Product Offers (UPPO) schemes. Information on the UIP and UPPO processes can be found at: www.defence.gov.au/casg/DoingBusiness/Industry/FindingOpportunities/



Contact CIOG

Directorate of Procurement and Contacting Services

CIOG.ProcurementAdvice@defence.gov.au

Postal Address

Chief Information Officer Group

Department of Defence

PO Box 7953

CANBERRA BC ACT 2610

www.defence.gov.au/cio



Australian Government

Department of Defence