CASE STUDY: Single Information Environment Security Architecture (SIESA) Delivery Team

Client:

Defence Chief Information Officer (CIO) Group

Timeframe:

February 2012 - April 2014

Area of expertise:

Strategy and Policy

Responsible for:

SIESA Project Delivery

Challenge

The Australian Defence Force (ADF) charged the CIO Group with delivering a Single Information Environment (SIE) to support and enable information and decision superiority.

Defence was undergoing a complex ICT transformation program. It had a number of competing priorities and time frames for delivery of capabilities that were already in development or were planned to contribute to Single Information Environment (SIE) security.

Due to this complexity an SIE Security Architecture (SIESA) was required to provide a clear strategy that would communicate and guide its multiple implementation projects, and to manage the associated and inter-related risks and challenges.

Therefore, the challenge was "*…to sufficiently secure the SIE to support and enable Defence's mission objectives with the ability to respond to an evolving threat environment*." (Greg Farr CIO Defence)

Approach

The SIESA is the means by which CIOG describes the future ICT security functional model, capabilities, and services, and the standards by which these are implemented. The SIESA is the foundation by which the CIO of Defence shall achieve the target state for security and secure the information and technology assets of Defence.

archTIS were able to define both the project scope and what security architecture meant to all the stakeholders by maintaining a very high level of engagement for the duration of project activities.

The SIESA consists of a suite of policies, principles and architectural artefacts and gave all stakeholders confidence that the SIESA would result in actual changes and improvements to the Defence security posture more broadly.

Outcomes

archTIS followed a top down architectural approach to ensure alignment between each layer of the organisation (Executive

through to Operations). This approach ensured that the completed SIESA delivered:

- A comprehensive security architecture that identified and applied 'Defence-in-Depth' controls to enable dynamic responses to changing threats;
- ICT security capabilities that are managed as a core part of service and system solution delivery;
- A trusted environment for integrated information sharing across Defence's architecture domains and the extended Defence enterprise;
- The technology and process patterns which implement the security function, and the means by which the ICT assets of Defence are secured;
- Seamless security to enhance the user experience and maintain accountability and compliance with legal and regulatory requirements; and
- The necessary balance between Defence's 'need-to-share' and 'need-to-know' requirements.

archTIS used our proprietary consulting methodology, drawing on standard architecture frameworks (SABSA, DODAF, Zachman), to ensure all stakeholders within the organisation had a common understanding of the SIESA, its application and benefits for securing the SIE.

Recognition

The SIESA was recognised as having "*radically improved Defence's understanding of ICT security capabilities and its ability to deliver required ICT security outcomes."* (Defence Awards Ceremony program, 2014). As a result, archTIS won the 'Outstanding Contribution to Security by Defence Industry' award at the 2014 Annual Defence Excellence in Security Awards Ceremony.