DEFENCE INNOVATION NETWORK

E: info@defenceinnovationnetwork.com
W: www.defenceinnovationnetwork.com

OFFICE AT:
Building 5B, Level 5, Room 25-26, 1 Quay St, Haymarket NSW 2000

Defence Innovation Network Grant Scheme: Pilot Project

Demonstration of an architecture for a future Defence Network

The Defence IT network (communications, compute and storage) is segmented by security classification into multiple networks; a state of affairs which has its origins in the management of information in the pre-Information Technology era rather than being designed for the Information Technology age.

This segmentation restricts the flow of information from producer to consumer which extends the operational decision-making cycle time and is fundamentally at odds with Defence's strategy of achieving, and exploiting, information superiority over an adversary; where information superiority is a combination of knowing more and being able to utilise that knowledge quicker and more effectively than the adversary.

CIO Group in Defence is responsible for the integrity of information managed within the network and invests significant resources in assuring the integrity of the discrete networks through the creation and maintenance of barriers to information flow between the different networks.

Providing information assurance through mechanisms which allowed information to flow from producer to consumer whilst ensuring that only consumers who had a need and authority to access information in their current context would be a significant enabler in allowing Defence to achieve real information superiority and maximise the benefits that Defence seeks to achieve through investment in up to date Defence capabilities such as 5th Generation air force platforms.

The question is two-fold; what would the Defence network look like if it were designed to facilitate information superiority and secondly how could CIO Group evolve the existing networks from the current to future state without compromising information assurance along the journey?

[Some] Specific questions that need addressing to design a future state Defence network:

1. Is the "zero trust" network model viable for Defence? Or a "low trust" variation?
2. Is encryption the answer? If so,
    a. Can software cryptography be used or are hardware cryptos required?
    b. What encryption algorithms should be used?
    c. Is Quantum Computing a threat, if so how is that threat treated?
    d. Does encryption have to be pervasive?
3. Should Defence have an enclosed network (i.e. not a public network)?
    a. What is needed to defend the boundary of the Defence network?
    b. What is needed to assure the availability of the network as a utility to Defence?
    c. What are the risks and mitigations for fixed, Wi-Fi and mobile (4G, 5G) networks specifically?

E: info@defenceinnovationnetwork.com
W: www.defenceinnovationnetwork.com

OFFICE AT:
Building 5B, Level 5, Room 25-26, 1 Quay St, Haymarket NSW 2000

4. What authentication mechanisms are required to provide a sufficient level of trust to allow an individual to access information?
    a. For different security classifications?
    b. For different user contexts?
5. What authorisation models are required? RBAC? ABAC?
6. How can legacy systems and applications be protected within the new network construct?
7. What authorisation models are required? RBAC? ABAC?
8. Are there relevant lessons to be learnt from Cloud concepts and providers?
9. What standards, certifications and accreditations are relevant?
10. What are the risks and benefits from having a single network in fixed and deployed environments specifically?

The approach would be to hypothesise what a future Defence network would look like and then challenge that from different perspectives to refine the vision and arrive at a target future state. Having defined a future state, approaches and techniques would then be developed to produce a roadmap for Defence to evolve forward from where they are to where they want to be.