POSITION DESCRIPTION

Position Title:	**Software and Systems Security Researcher**
Position Reference Number:	R&ICEWD009b/ECR014b
Division	Cyber and Electronic Warfare Division
Position Classification:	S&T3-4 (APS4/5-6)
Position Location:	Edinburgh, SA
Security Level:	Negative Vetting 1 minimum
Enquiries:	Mark Beaumont, Mark.Beaumont@dst.defence.gov.au, (08) 7389 7436

Academic Disciplines

Aerospace/ Aeronautical Engineering, Naval Architecture	Chemical, Radiological, Biological, Food sciences	Materials Science
Computer Sciences, IT, Software Engineering, Telecommunications	Mathematics and physics	Psychology and Social Sciences
Mechanical and Mechatronic Engineering (including robotics)	**Electronic/ Electrical Engineering**	Other

Position Overview

The candidate will be part of an S&T team undertaking applied research to ensure that Australian Defence has a secure platform for cyber warfare. This includes supporting the security analysis of Military Cyber systems and the development, experimentation and transition of new vulnerability analysis tools.

The role calls for an active researcher, or research engineer, with a background in computer science or engineering and a bent for cyber security who can apply their skills to undertake challenging research on the cyber security of military and related embedded systems.

The role will provide an array of S&T challenges within cyber security and operations in the military context. There exists the opportunity to work closely with Australian and international research partners, Defence clients and cyber security experts.

The successful candidate will be supported with training in aspects of cyber security as required, and encouraged to further develop their scientific or engineering expertise.

Position Duties

Working individually or as part of a multi-disciplinary project team, the candidate will undertake challenging research on the cyber security of military and related embedded systems including:

- Contribute to applied research and development of novel tools and techniques for mitigating the complexity in military cyber systems:
  - Development of trustworthy security devices and applications to ensure correct operation of critical systems.
  - Development of tools for assisting the vulnerability analysis of military cyber systems.
  - Development of tools for software reverse engineering, software vulnerability analysis, and verification of security critical functionality
- Undertake security analysis and assessment of military system software and embedded components.
- Prepare publications, present outcomes, demonstrate technologies and interact with clients and stakeholders.
- Maintain up to date knowledge in chosen disciplines and broaden knowledge across cyber security and operations.

Enhance S&T capability through collaboration with other DST Group teams, academia, industry and other research agencies.

Other Requirements

The applicant will have a high level of written and oral communications skills, and will be able to demonstrate this by reference to both written products and examples of oral communications (e.g. presentations, mentoring, and knowledge transfer) in the technical domain.