

# Ensuring Defence's sec

**The Defence Security Authority's (DSA) is known for conducting security clearance assessments for Defence military and civilian personnel. However, much of DSA's other roles and responsibilities are less known, yet are crucial to the success of Defence capabilities and operations.**

Some of these activities include developing protective security policy, providing security advice, validating security practices, and measures to protect Defence information and assets. DSA also establishes and maintains international security instruments and investigates serious security incidents.

The following DSA staff profiles demonstrate the diverse and interesting work carried out across DSA.

**Antoinette Perceval, Principal Security Adviser, Weapons Munitions and Explosives Team**



I am a member of the DSA Weapons Munitions and Explosives (WME) Team, which was established following the WME Security Performance Audit in August 2007. My role is to conduct security performance reviews that analyse and assess the effectiveness of WME security policy, standards and practice.

By identifying Defence-wide, systemic WME security issues and recommending improvements, the reviews assist Defence commanders and managers at all levels to apply security policy, programs and response plans more effectively.

The reviews that I conduct have been identified through Defence and IS&IP's strategic priorities and the DSA Business Plan, or subjects that have been judged by Group Heads and Service Chiefs to be high risk or critical for Defence. I also conduct security incident trend analysis to guide future security performance reviews.

**Graham (Doc) Chinner, Assistant Director, Technical Surveillance Countermeasures**

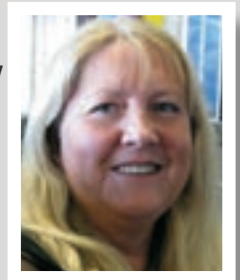
As a team leader in the Technical Surveillance Countermeasures (TSCM) section it is my role to ensure the section develops and implements ways to reduce the risk of sensitive Defence audio and video information being compromised.

To carry out this important role, my team conducts assessments on Defence sites across Australia. These assessments involve determining risk and technical vulnerabilities of a site, as well as assessing the volume, value and type of information being processed at that location.

We then apply risk management to the assessment, and a technical inspection plan is developed and executed. Each inspection is conducted with a variety of electronic, mechanical and optical equipment.

If you ever get the opportunity, be sure to attend one of our technical security awareness presentations (more info is available from the DSA's Technical Surveillance and Countermeasures team). Tailored to suit a variety of audiences, the aim of the presentation is to help you understand the need for good security practices and rules. You'll experience a hands-on demonstration and learn how information can be extracted from a controlled space to a recovery point using a wide range of devices.

**Wendy Norris, Assistant Director, Security Incident Centre**



The Security Incident Centre (SIC) receives and assesses reports of security incidents in Defence.

This includes all incidents related to WME and controlled items.

We compile various statistical reports in relation to security breaches, WME and controlled item incidents in Defence.

As a member of Defence, it is your responsibility to familiarise yourself with Defence Security Policy and always be security conscious. Most security breaches reported to the SIC relate to the way people handle classification information, particularly on Defence ICT systems.

All security incidents except for minor incidents, must be reported to the SIC within 24hrs of the incident occurring. This does not negate the normal reporting of incidents to your Unit Security Officer.

SIC can be contacted by emailing:

- DRN security.incidentcentre@defence.gov.au
- DSN security.incidentcentre@jcsd.defence.gov.au

Or via telephone:

- 02 6266 4520,
- 0416 060 347 (AH),or
- 02 6266 2984 (UNCLASSIFIED fax).

**All minor security incidents must be forwarded to the regional DSA offices within 48hrs.**

# urity

**Paul Wilkinson,  
Assistant  
Director –  
Positive Vetting,  
Directorate of  
Vetting**



The most frequently asked questions at DSA are related to Positive Vetting.

Defence personnel who require access to compartmented information, Top Secret IT systems or who regularly deal with a large volume of Top Secret material, are required to hold a Top Secret Positive Vetting (TSPV) security clearance. This generally includes all personnel working in the Defence intelligence agencies, intelligence-related employment categories, and many ADF personnel on operational deployments.

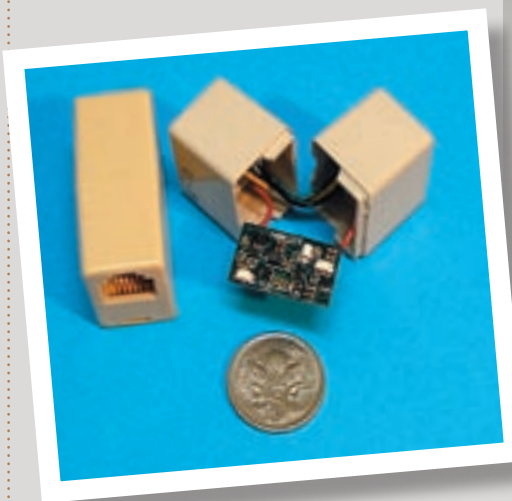
The security vetting for a TSPV security clearance is intrusive, rigorous and lengthy (approximately six months), in comparison to lower level security clearance processes. The aim of the initial security clearance vetting process is to establish identity and determine the suitability of a clearance subject to hold a specific level of security clearance. The monitoring of a clearance subject's continued suitability to hold a security clearance is a fundamental aspect of good personnel security practice. At the TSPV security clearance level, a security vetting aftercare regime is applied to ensure that TSPV clearance holders remain suitable to have access to highly classified resources.

**For more information on vetting please visit <http://intranet.defence.gov.au/dsa/>.**

**Edward Huddy, Assistant Director,  
Directorate of Security Operations,  
Planning and Coordination**

I oversee DSA's role in the implementation and management of the Australia-US Treaty concerning defence trade cooperation. Under the Treaty, DSA is responsible for the implementation and management of security arrangements for the Australian Community. The 'Australian Community' is the Australian Government facilities and non-Government (private sector) entities, who will be able to trade Defence articles with the US using the provisions of the Treaty.

The Treaty requires that members of the Australian Community demonstrate a need to access the Defence articles which can be traded using Treaty provisions. Therefore, each potential member of the Australian Community will need to apply for entry and demonstrate their need for access.



## Wendy's top five security tips

- Understand security policy and report all breaches.
- Understand what security classified information is, and follow the storage, handling and transportation requirements designed to protect it.
- Understand and apply the Need-To-Know principle.
- Do not share your passwords; they protect you and Defence.
- Be security aware at close of business; check your workspace.

**LEFT: Example of a hidden communication device - a telephone transmitter in a phone connector.**