

UNCLASSIFIED



Australian Government

Department of Defence  
Defence Science and  
Technology Organisation

# DHS Cyber Security Division Broad Agency Announcement 2012 PI Meeting

## Australian Presentation

National Security Science & Technology Centre  
DSTO, Australia

*David McIlroy, Head NSSTC Canberra*  
*david.mcilroy@dsto.defence.gov.au*

UNCLASSIFIED

**DSTO**



Chief Defence Scientist  
Dr Alex Zelinsky



Deputy CDS  
Platform & Human Systems  
Dr Ian Sare

Air Operations Division  
Chief: Dr Todd Mansell

Air Vehicles Division  
Chief: Dr Ken Anderson

Human Protection &  
Performance Division  
Chief: Dr Simon Oldfield

Maritimes Operations  
Division  
Chief: Dr John Riley

Maritime Platforms Division  
Chief: Ms Janis Cocking

Scientific Engineering  
Services  
Mngr: Mr Robert Weimann

Chief Operating Officer  
Division  
COO: Dr Len Sciacca

Group Finance Officer  
Branch  
GFO: Mr Martyn Taylor

Science Strategy  
Policy Branch  
DG: Dr Richard Davis

Projects &  
Requirements Division  
Chief: Mr Jim Smith

Science Industry &  
External Relations  
Branch  
AS: Mr Alan Gray

Science Corporate  
Information Services  
Deputy CIO:  
Dr Tony Hookins



Deputy CDS  
Information & Weapon Systems  
Dr Warren Harch

Command, Control,  
Communications  
& Intelligence Division  
A/Chief: Dr Jackie Craig

Electronic Warfare &  
Radar Division  
A/Chief: Dr Andrew Shaw

Intelligence, Surveillance &  
Reconnaissance Division  
Chief: Dr Tony Lindsay

Joint Operations Division  
Chief: Dr Jennifer Clothier

Land Operations Division  
Chief: Mr Steve Quinn

Weapons System Division  
Chief: Dr Bruce Ward

Chief Systems Integration Officer  
Mr Paul Amoy

National Security Science and  
Technology Centre  
Exec Director: Dr John Percival



# Background – DSTO Support to National Security

**Prior to 2003:** *Ad hoc S&T support through Defence*

**2004 PM's directive:** *“to develop DSTO's counter terrorism S&T capability to support civilian agencies and the ADO's ability to respond to terrorist threats”*

**2006 Ministerial approval for expanded DSTO mandate**

**2007 Counter Terrorism & Security Technology Centre (CTSTC) Established**

**2009 Defence White Paper**

- *endorsed DSTO National Security Program*
- *acknowledged benefits to Defence*

**2012 (1 Feb) Transfer of NS S&T Functions from PM&C to DSTO**

**2012 (1 Apr) CTSTC renamed to the National Security Science & Technology Centre (NSSTC)**



DWP Key S&T Areas for non defence:

- CBRN
- Explosives
- Intelligence
- Cyber-security

# National Security S&T Centre (NSSTC)

## *MISSION*

*To coordinate and develop science and technology to enhance whole-of-government national security*



Implement national security S&T policy and coordination processes



Manage the DSTO National Security research program



Foster international national security research collaboration



Lead and undertake analysis of whole-of-government national security systems



Integrate counter-terrorism technologies to benefit Defence and civilian agencies

# National Security 'International' Program

*NSSTC holds Responsibility for three international agreements:*

- **CTTSO MOU, 10 year duration**
- **DHS Treaty, no expiry date**
- **UK Home Office MOU, 10 year duration**

*Many S&T Providers, including DSTO*  
*High leverage*

*Defence funding was allocated to the transfer of former NSST Functions (reduced resources)*



# NSSTC Structure

August 2012



**Dr John Percival**  
Executive Director

**Dr Jolanta Ciuk**  
Executive Officer

**Ms Heather Oermann**  
Executive Support Officer

*Canberra Node*  
NS S&T Requirements  
NS Agency Liaison  
Intl. Program Mgt

**NS Programs Coordination**  
Business Commercialisation Office

**Strategic Risk Research**  
Resource Manager IWS

**CT technologies**

**Ms Tori Marshall**  
Defence Legal

**Mr David McIlroy**  
Head, NSST Canberra

**Dr Wayne Hobbs**  
Head, NS Programs

**Dr Rick Nunes-Vaz**  
Head, CT & Security Analysis

**Dr John Asenstorfer**  
Head, CT Technologies

**Vacant**  
DSTO Secondment to AGD

**Vacant**  
DSTO  
Program Manager

**Dr Sarah Benson**  
AFP Secondment  
Program Manager

**Mr Ross Ackland**  
CSIRO Secondment  
Program Manager

**Mr Sean Cheng**  
International  
Project Coordinator

**Divisional S&T Leads**

**Dr Leung Chim**  
Senior Research Scientist

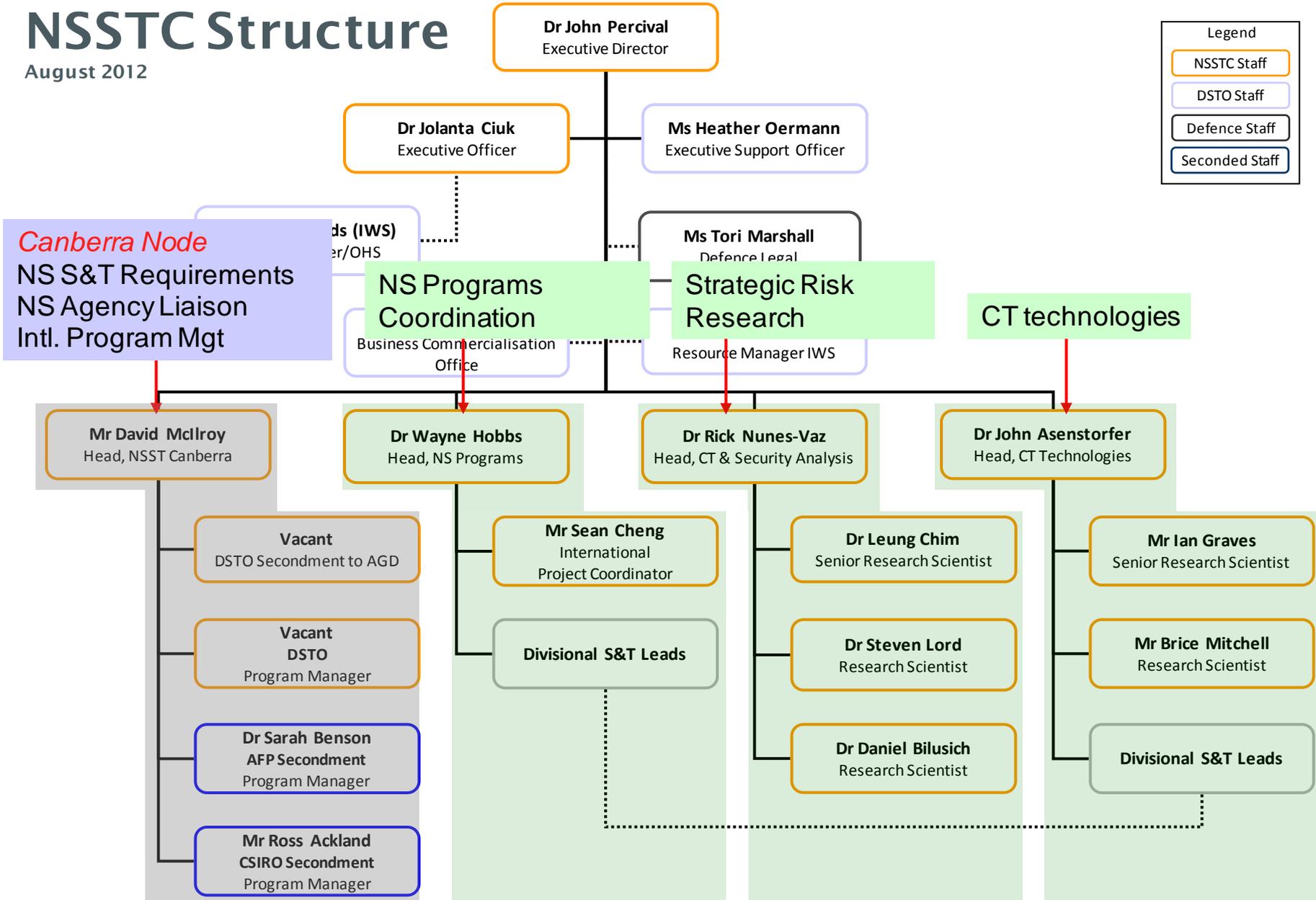
**Dr Steven Lord**  
Research Scientist

**Dr Daniel Bilusich**  
Research Scientist

**Mr Ian Graves**  
Senior Research Scientist

**Mr Brice Mitchell**  
Research Scientist

**Divisional S&T Leads**





## *Cyber-Security Conducted under PA08-0011*

### *TA01 Watchdog system for Internet routing (Border Gateway Protocol)*

- Researcher: Colorado State Uni*
- Aim: To develop a system for monitoring Australian Critical Infrastructure as part of the larger cyber security and internet monitoring effort for both the US and Australian Governments, and to increase monitoring connectivity in Australia and the larger Asia Pacific region. Aus lead agency: AGD (CERT). Work strongly supported by AGD, ACMA and DHS.*
- Status: AUS considers the work to be going well. A future phase using geo-tagging may have 'cross-interest' to AGD's critical infrastructure area (CIPMA)*



## *TA02 – Next generation DNS Monitoring (Botnet)*

- Researcher: Georgia Inst of Tech*
- Aim: To develop a tool to assist in determining the origin of botnet attacks, and to develop a system for Australia to detect DNS covert channels. Ongoing project. Due for conclusion in FY13. Aus lead agency: AGD (CERT)*
- Status: DHS comment invited. Progress reporting is notably minimalistic*



## *TA03 – Economics of Cybercrime*

- *Researcher: Carnegie Mellon Uni*
- *Aim: Ongoing project focussed on understanding and disrupting the economics of cybercrime. Includes developing new theories and models of cybercrime and its social dimensions. Australian Federal Police (AFP) interest.*



## *TA04 – Malicious Overlay Networks*

- *Researcher: Georgia Inst of Tech*
- *Aim: Ongoing Project. Development of a Federated Malware Analysis System (FMAS) and real time analysis of dynamic information to attribute malware to a Botnet. Defence and AGD stakeholders*



## *Proposed Projects*

### *Equipment Vulnerabilities*

- *Tentative interest from Defence for Edith Cowan University Security Research Institute to look at equipment (unspecified) vulnerabilities. AGD(CERT) another stakeholder*

### *Flash Memory Remanence*

- *Adelaide Uni proposal - Validating sanitisation procedures for flash memory chips*
- *Aus Defence interest, including DSTO. UK interest*



## *Proposed Projects*

### *Postquantum Cryptography and Secure Cloud Storage*

- Uni of Wollongong - Development of postquantum cryptography and its applications to secure cloud computing. Seeking a follow-on to previous PM&C NSST domestic funded research*
- Macquarie Uni – also proposing capability in secure cloud data storage*

*Questions?*

