Program
&
Conference Handbook

Program: Day 1—Tuesday 10 November 2015.......................................................... 2
Program: Day 2—Wednesday 11 November 2015 .................................................. 3
Program: Day 3—Thursday 12 November 2015.................................................... 4
Session Abstracts: Day 1—10 November 2015...................................................... 5
Session Abstracts: Day 2—11 November 2015...................................................... 10
Session Abstracts: Day 3—12 November 2015...................................................... 16
<table>
<thead>
<tr>
<th>Time</th>
<th>Session 1</th>
<th>Session 2</th>
<th>Session 3</th>
<th>Session 4</th>
<th>Session 5</th>
<th>IEEE STREAM</th>
<th>Session 6</th>
<th>INDUSTRY STREAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>07:30am</td>
<td>Breakfast Session: Exhibition open and coffee available (Assistant Minister for Defence, Group Heads, and Service Chiefs in attendance)</td>
<td>Session 1.2 Plenary Session: Opening Session</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9:00am</td>
<td>Session 1.2 Plenary Session: Opening Session</td>
<td>Welcome: Professor Michael Frater, Rector UNSW Canberra and Dr Peter Lawrence, Chief Information Officer, CIOG</td>
<td>Opening Session</td>
<td>Welcome: The Honourable Stuart Robert MP, Assistant Minister for Defence</td>
<td>Keynote Address: Dr Peter Lawrence, Chief Information Officer, CIOG</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00am</td>
<td>Morning Tea</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.30am</td>
<td>Session 1.3a Plenary Session: CIO Session</td>
<td>Keynote Address: ICT Strategy and the Way Ahead: Mr Aiyaswami Mohan, Chief Technology Officer, CIOG</td>
<td>Keynote Address: The Infrastructure Journey: AVM Andrew Dowse, Head ICT Operations Division, CIOG</td>
<td>Keynote Address: The Infrastructure Journey: Ms Julie Dunlap, Vice President, Australian Programs, Lockheed Martin</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:30pm</td>
<td>Lunch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.30pm</td>
<td>Session 1.4a Product Brief: Security Hardening—Reducing the Cyber Attack Surface (Mr Clive Reeves, Telstra)</td>
<td>Session 1.5a Product Brief: Where You Want When You Want (Mr “D” D’Ambrosio, Q3b Networks)</td>
<td>Session 1.6a Update: HP (Mr TBA)</td>
<td>Paper 1: System Dynamics Modelling of Situation Awareness</td>
<td>Paper 1: An Onion Approach to Cyber Warfare Training</td>
<td>Paper 1: Serving up Data Files to Multiple Classified Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.30pm</td>
<td>Session 1.4b Update: Business Architecture—Enabling Management (Mr Christopher Rodrigues Macias, CIOG)</td>
<td>Session 1.5b Product Brief: Leveraging the Complementary Capability of MGS and Commercial Satcom (Mr Andy Start, Inmarsat)</td>
<td>Session 1.6b Update: TBA (Mr TBA, NGC)</td>
<td>Paper 2: On the Evaluation of Military Simulations: Towards A Taxonomy of Assessment Criteria</td>
<td>Paper 2: On the Evaluation of Military Simulations: Towards A Taxonomy of Assessment Criteria</td>
<td>Paper 2: Preventing Data Spills from Classified Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.30pm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.00pm</td>
<td>Session 1.4c Update: Amphibious Architecture Developments (CDRE Stephen Woodall, VCDF, Mr Christopher Rodrigues Macias, CIOG &amp; Mr Colin Keith, ROMAC)</td>
<td>Session 1.5c Product Brief: Skynet 5—Military Satcom over Asia-Pacific Region (Mr Simon Barker, Airbus Defence and Space)</td>
<td>Session 1.6c Product Brief: TruNet™ Seamless Networked Enabled Communications for the Air Land and Sea (Mr Cameron McDonald, Rockwell Collins)</td>
<td>Paper 1: Enhancing Wireless Communications with Software Defined Networking</td>
<td>Paper 1: Simultaneous X and Ka Band Maritime Satcom Terminal Supporting Both Military and Commercial Ka Band Communications</td>
<td>Paper 1: Simultaneous X and Ka Band Maritime Satcom Terminal Supporting Both Military and Commercial Ka Band Communications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.00pm</td>
<td>Welcome Networking Drinks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Exhibition runs from 7:30am to 6:30pm (open to exhibition-only registration from 1:30pm to 4:30pm) / IEEE Stream (Refereed papers) co-sponsored by IEEE
Day 2—Wednesday 11 November 2015

<table>
<thead>
<tr>
<th>Time</th>
<th>Session 2.1</th>
<th>Product Brief (Ballroom): Senetas and Nextgen Group Partner to Deliver ‘Defence-Grade’ State of the Art Secure Data Centre and Networks Services, Mr Julian Fay, Chief Technology Officer, Senetas Corporation</th>
</tr>
</thead>
</table>
| 9.00am | Session 2.2 | Plenary Session: Navy, Army, Air Force CIS Interoperability  
Moderator: AVM Andrew Dowse, Head ICT Operations Division, CIOG  
Keynote Address: RADM Michael van Balen, Deputy Chief Navy  
Keynote Address: MAJGEN Fergus McLachlan, Head Modernisation and Strategic Planning – Army  
Keynote Address: AIRCDRE Stephen Osborne, Director-General Strategy and Planning – Air Force |
| 10.30am|             | Morning Tea |
| 11.00am| Session 2.3a| Plenary Session: Capability Developments  
Keynote Address: AVM Mel Hupfeld, Head Capability Systems, CASG  
Keynote Address: RADM Peter Quinn, Head Joint Capability Coordination, VCDF Group  
Keynote Address: RDML Kathleen Creighton, US PACOM J6  
Keynote Address: Mr Victor Vae’au, CIO NZDF |
| 12.30pm| Lunch       | Session 2.3b Product Brief: TBA (Berkeley IT) |
| 1.30pm | Session 2.4a| Update: MNIS Strategy and Capability Overview  
(Mr Ewart Challis, Director Multinational Relations and Interoperability) |
|        | Session 2.4b| Update: Changing the Face of Cyber Security  
(Mr Richard Brown, Cogito Group) |
| 2.00pm | Session 2.5a| Product Brief: Managing people and Processes Through Roles  
(Mr James Miley, Myriad Technologies) |
|        | Session 2.5b| Product Brief: The Case for Secure Mobility in Defence  
(Mr Jon Green, Aruba Networks) |
| 3.00pm |               | Afternoon Tea |
| 4.00pm | Session 2.6a| Update: Defence Spectrum Strategy  
(Mr Alex Wright, Defence Spectrum Office, CIOG) |
|        | Session 2.6b| Update: Government Spectrum Review—Implications for Defence  
(Mr Alex Wright, Defence Spectrum Office, CIOG) |
|        | Session 2.7a| Product Brief: Next Generation Mobile Intelligence: Dynamic Collaboration Solutions  
(Mr Graeme Stanley, Motorola Solutions) |
|        | Session 2.7b| Update: Centralised Processing—Transformation  
(Ms Julie Bance, Lockheed Martin Australia & Ms Janice Law, CIOG) |
|        | Session 2.8a| INDUSTRY STREAM  
Paper 1: Symmetrical Data Link for Burst Mode Transmission  
Paper 2: Validation of MUF and FOT Parameters for Plain, Mountainous and Sea Region |
| 4.00pm | Session 2.8c| Tutorial: Wireless Backhaul—A Primer on Microwave and Satellite Communications  
(Mr Rowan Gilmore, EM Solutions) |
|        |             | INDUSTRY STREAM  
Paper 1: Miniaturized Wideband Branch-Line Hybrid Coupler with Four Pine Shape Capacitive Effect  
Paper 2: Design and Simulation of Digital Down Converter for SQFSK Wideband Heterodyne Receiver |
| 7.00pm |               | Conference Dinner (7:00pm for 7:30pm) |

Exhibition runs from 7:30am to 5:00pm (open to exhibition-only registration from 1:30pm to 5:00pm)
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>07:30am</td>
<td><strong>Session 3.1</strong> Breakfast Session—Exhibition open and coffee available</td>
<td></td>
</tr>
</tbody>
</table>
| 9:00am | **Session 3.2** Plenary Session: Defence Cyber  
Keynote Address: Mr Chris Brookes, Executive Director Cyber Security, I&S Group  
Keynote Address: Mr Lindsay Morgan, A/Assistant Secretary ICT Security, CIOG  
Keynote Address: WGCDR Michael Reidy, Deputy Director Defence Cyber Coordination Office, VCDF Group |
| 10:30am| Morning Tea |
| 11:00am| **Session 3.3a** Plenary Session: SecureCanberra Track  
Welcome Address: TBA  
Keynote Address: TBA  
Keynote Address: TBA  
Keynote Address: Prof. Jill Slay, Australian Centre for Cyber Security, University of New South Wales |
| 12:30pm| Lunch  
**Session 3.3b** Product Brief: TBA (Mr TBA) |
| 1:30pm | **Session 3.4a** SecureCanberra Track  
1.  
2.  
**Session 3.5a** Product Brief: Harris Next Generation C2ISR Capabilities  
(Mr Adrian Craven, Harris Software Systems)  
**Session 3.6a** Tutorial: Document and Records Management in SharePoint  
(Mr James Milne, Myriad Technologies)  
**Session 3.7a** Product Brief: TBA  
(Mr TBA, TBA) |
| 2:30pm | **Session 3.4b** SecureCanberra Track  
1.  
2.  
**Session 3.5b** Product Brief: Icom Australia: For Everything in Radio  
(Mr Grant Fernando, Icom Australia)  
**Session 3.6b** Tutorial: Replication in the Field  
(Mr James Milne, Myriad Technologies)  
**Session 3.7b** Product Brief: TBA  
(Mr TBA, TBA)  
**Session 3.8a** Tutorial: Establishing a Flexible, Open Cyberinfrastructure Framework for Virtual Organizations  
(Dr Morcosu Massoud, Cairo University) |
| 3:30pm | Afternoon Tea |
| 4:00pm | **Session 3.4c** SecureCanberra Track  
1.  
2.  
**Session 3.5c** Update: New Antennas for New Battlefields: EW Antennas—A Platform Capability  
(Mr David Benchoam, Benelec)  
**Session 3.6c** Tutorial: Building Electronic Forms and Workflows to Streamline your Business Processes  
(Mr James Milne, Myriad Technologies)  
**Session 3.7c** Update: TBA  
(Mr TBA, TBA) |

Exhibition runs from 7:30am to 1:30pm (NO exhibition-only registrations available)
Session Abstracts: Day 1—10 November 2015

1.1 Breakfast Session

The Exhibition is open and coffee is available in the Exhibition Hall.

1.2 Plenary Session—Opening Session

Welcome: Professor Michael Frater, Rector UNSW Canberra and Dr Peter Lawrence, Chief Information Officer, CIOG
Conference Opening: The Honourable Stuart Robert MP, Assistant Minister for Defence
Keynote Address: Dr Peter Lawrence, Chief Information Officer, CIOG

1.3a Plenary Session: CIO Session

Keynote Address: ICT Strategy and the Way Ahead: Mr Aiyaswami Mohan, Chief Technology Officer, CIOG
Keynote Address: AVM Andrew Dowse, Head ICT Operations, CIOG
Keynote Address: Ms Julie Dunlap, Vice President, Australian Programs, Lockheed Martin

1.3b Lunch Session Product Brief: TBA

Presenters: Mr TBA, TBA

1.4a Product Brief: Security Hardening – Reducing the Cyber Attack Surface

Presenters: Mr Clive Reeves, Chief Information Security Officer, Defence Engagement, Telstra

ICT systems are vulnerable to attack through a range of threat vectors.

Security hardening can significantly improve the security posture by assessing the threats and then implementing a range of hardening techniques to reduce the attack surface and mitigate the security risks. Hardening a system involves a range of techniques. These may not completely prevent all successful attacks but it will significantly reduce the risk of compromise, minimise the likelihood of lateral movement, and provide an opportunity to detect and respond to an attack as soon as possible.

This ‘case study’ will provide an example of how threats can be used to derive high level risks for a large and complex ICT system; how hardening techniques can be applied (including practical examples of challenges that arise in achieving successful outcomes); and how these security controls can aligned to the engineering lifecycle and build process to achieve the best possible outcome.

1.4b Update: Business Architecture – Enabling Management

Presenter: Christopher Rodrigues Macias, Assistant Secretary Enterprise Architecture Branch, CIOG

The Defence Business Reference Architecture has been created to provide a framework for officers and executives to develop and manage Defence. To achieve this it must enable discussion of Defence capabilities, services, information and organisations between military commanders and managers of enabling services.

In the emerging Defence environment, information assets are increasingly the lifeblood of Defence business. Defence knowledge worker’s feedstock of documents, journals, newspapers, legislation and policy has meant an enormous research effort being associated with most tasks. The Digital Age has struggled to make headway in this challenge for military and public servants.

In recent years, we have been bombarded with Big Data hype but are we looking at the problem the wrong way? Is the challenge of having the right information (data) going to get worse with the emerging Internet of Things? While these are interesting questions; in this update we will constrains our focus and explore these issues and how the Defence Business Reference Architecture may assist.
We explore how enterprise, business and process architecture perspectives can assist Defence in coping with the challenges outlined above. These architectures which tend to be overlooked, can deliver value and enable substantial performance improvements. While also providing guidance that supports other architecture development such as project architectures. This update will also reference a number of initiatives “in-flight” across Defence to support the value of the Defence Business Reference Architecture.

1.4c Update: Amphibious Architecture Developments

Presenter: CDRE Stephen Woodall, VCDFG, Mr. Christopher Rodrigues Macias, CIOG, and Mr. Colin Keith, RDA

Australia’s ability to conduct amphibious operations will be significantly enhanced with the delivery of platforms such as the Landing Helicopter Dock, new sealift and heavy landing craft (Defence White Paper, 2009). The introduction of this enhanced capability provides an opportunity for the ADF to explore the networking of the joint warfighter, at the tactical level, as part of a broader integrated force.

To support this endeavour, and to ensure that a consistent approach is used in preparing for, planning and conducting amphibious operations, the Vice Chief of the Defence Force Group (VCDFG) have joined together with the Chief Information Officer Group (CIOG) to develop an architecture that describes the desired or Objective C4I Capability for amphibious operations. Indeed, this work will shape the remediation of both current fit and shorter term C4I systems’ acquisitions in the ship and ashore, while concurrently paving the way for joint force design of both amphibious and broader related joint C4I capabilities.

This presentation will describe the objectives of the architecture, how it was developed by drawing together existing material, and how a model of a complex space such as amphibious operations, can be harvested for wider programmatic and portfolio use. The new Joint Amphibious Capability will potentially provide a pattern that can be replicated in other joint warfighting contexts.


1.5a Product Brief: Product Brief: Where You Want When You Want

Presenter: Mr “D” D’Ambrosio, EVP, Government Solutions, O3b Networks

Update to O3b Networks Medium Earth Orbit (MEO) system and how the government(s) agencies are conducting test and evaluation (T&E) into how to use the system. O3b Networks provides lower latency and higher throughput than GEOs and is an enabler for a number of system (4G/LTE) and applications that cannot perform over GEOs.

1.5b Product Brief: Delivering Increased Operational Capability at Reduced Cost by Leveraging the Complementary Capability of WGS and Commercial Satcom

Presenter: Mr Andy Start, President, Global Government, Inmarsat

Governments globally are facing increasing operational challenges and must meet these challenges under increasing fiscal constraints. Using a series of scenarios and case studies, the presenter will illustrate how using the latest e-enablement techniques, government leaders can deliver greater operational effect at less cost. Giving specific examples of integrating secure applications with the latest commercial satcom technology and military systems such as WGS, the presenter will show how land, sea and air capabilities can be seamlessly integrated to drive powerful operational effect.

1.5c Product Brief: Skynet 5—Military Satcom over Asia-Pacific Region

Presenter: Mr Simon Barker, Asia Business Development, Airbus Defence and Space

Airbus Defence and Space owns and operates the hardened Skynet X-band satellite constellation of eight satellites and the ground network to provide all Beyond Line of Sight (BLOS) communications to the UK Ministry of Defence. The contract also allows other NATO and allied governments to use the Skynet system to augment their existing services. Airbus Defence and Space also leases the X-band hosted payload on Telesat’s Anik G1 satellite which covers the Americas and parts of the Pacific including Hawaii and Easter Island.
The move to Skynet 5A will enable delivery of protected and secure satcom services in the new coverage footprint from mid-2015.

1.6a Update: HP
Presenter: TBA, HP
TBA

1.6b Update: NGC
Presenter: TBA, NGC
TBA

1.6c Product Brief: TruNet™ Seamless Networked Enabled Communications for the Air Land and Sea
Presenter: Mr Cameron McDonald, Principal Marketing Manager - Asia Pacific, Rockwell Collins

TruNet™ from Rockwell Collins is the first software defined network communications solution – including ground, airborne and handheld radios, advanced networking waveforms, apps, ancillaries and services – to ensure secure connectivity between ground, airborne and sea elements. Flexing to your unique mission requirements, TruNet gives you complete control of your networked communications across the entire battlespace.

TruNet gives your ground, airborne and maritime forces the power to network as never before, securely and in real time. Its ground breaking capability puts seamless interoperability in your arsenal. TruNet enables the secure sharing of critical data, image, voice and video communications across all domains in your battle space. Whether your forces are operating alone or with joint or coalition elements, stay connected and aware, no matter their mission, location or platform.

TruNet’s Airborne (AR), Ground (GR) and Handheld (HH) series software defined radios are small, light and powerful. And, TruNet enables your developers to easily tailor the system – from a few handheld radios to a complete ground-air-sea network – to meet your mission needs. TruNet’s robust and reliable radios feature multiple narrow and wideband waveforms and open architecture, as well as apps and ancillaries. This provides maximum flexibility, usability, easy integration with legacy waveforms and continuous readiness for cost-effective technology advancement.

1.7a Refereed Papers—IEEE Stream

Paper 1: System Dynamics Modelling of Situation Awareness
Author: Rudolph Oosthuizen
Abstract. One of the requirements for effective Command and Control is good situation awareness. As situation awareness is a complex phenomenon due to social and cognitive interaction factors, its modelling, prediction and calculation can be difficult. The feedback loops and delays in the Command and Control system also contribute to the complex dynamic behaviour. This paper will build on existing situation awareness models to develop a System Dynamics model to support a qualitative analysis of key situation awareness variables through simulation

Author: Mario Golling, Robert Koch, Peter Hillmann, Volker Eiseler, Lars Sittemert, & Andreas Rekker
Abstract. In the area of military simulations, a multitude of different approaches is available. "Close Combat Tactical Trainer", "Joint Tactical Combat Training System", "Battle Force Tactical Training" or "Warfighter's Simulation 2000" are just some examples within the history of the large DoD Development Program in Modelling and Simulation, representing just a small piece of the variety of different solutions. Very often, individual simulators are sometimes very different and so it is often very difficult to classify military simulations even for experienced users. This circumstance is further boosted due to the fact that it in the field of military simulations - unlike in other areas - no general classification for military simulations exists. To address this shortcoming, this publication is dedicated to the idea of providing a first contribution to the development of a commonly accepted taxonomy in the area of military simulations. To this end, the problem field is structured into three main categories (general functional requirements for simulators, special military requirements for simulators and non-functional requirements for simulators). Based upon that, individual categories are provided with appropriate classes. For a better understanding, the taxonomy is used for a concrete example (NetLogo Rebellion).
Paper 1: Autonomy and Self-Organisation for Tactical Communications and Range Extension

**Author:** Robert Hunjet

**Abstract.** During operations, networks are typically analysed in terms of metrics such as throughput, delay and connectivity. Analysis and optimisations can be carried out on these metrics to achieve better networks; however, such approaches rely on strong processing power and a substantial amount of data collection. This may pose a problem as processing power is related to the cost of the platform, and data collection is a substantial overhead in the bandwidth constrained tactical space. This paper examines self organisational rules which operate without the passing of large amounts of data or the need for optimisation. These rules are shown to produce emergent behaviours which may be applicable to Military operations. Applicability to the fields of logistics, sensor networks, surveillance and range extension is discussed. Simulations yield encouraging results when self organising techniques are implemented to provide range extension.

Paper 2: Capacity Planning for Tactical Wireless Mesh Networks

**Author:** Matthew S Britton & Andrew Coyle

**Abstract.** Predicting the capacity of wireless mesh networks is difficult, due to the complex interaction of various layers such as the radio environment, media access protocols, network protocols and, traffic load and types. When modelling and simulation takes into account the interaction of all these factors, it can facilitate insights into anticipated network behaviour. These insights can be used to more effectively plan the deployment of the wireless network. In this paper we present a modelling and simulation approach which captures these aspects, and present results which demonstrate the types of insights this approach can provide, the most important being traffic capacity. When traffic capacity can be anticipated, various planning and operational decisions can be made with much more certainty.

Paper 1: Enhancing Wireless Communications with Software Defined Networking

**Author:** Marian Mihailescu, Hung Xuan Nguyen & Michael Webb

**Abstract.** In defence and emergency operations, integration between multiple wireless networks offers the choice of selecting the connection best suited to the type of information transferred, while at the same time expanding the coverage area in areas where only certain networks are available. Without effective command and control systems, response units at the operational edge, where critical real time information is generated and consumed, become "information islands". Controlling network traffic at higher echelons, in order to make better use of the limited network bandwidth available, improves the situational picture at the control centre and competence of emergency response units on the field. Traffic prioritization, remote network control, and multiple radio integration are three important criteria we are considering in the design of a two-level hierarchical software defined networking architecture for wireless networks, which expand on other SDN properties such as network agility, scalability, and programmability. We have built a prototype with multiple radio interfaces that can provide backhaul for response units by selecting the interface with the highest available throughput, where both policies and configuration can be programmed remotely. Even if our primary use case is geared towards emergency services, military communications challenges share many of the characteristics of emergency operations.

Paper 1: An Onion Approach to Cyber Warfare Training

**Author:** Daniel Clark

**Abstract.** This paper outlines an approach to cyber warfare training based on incremental exposure to a coherent set of foundation knowledge elements set within an operational context. The information in the paper is based on practical experience in providing cyber warfare training and observed behaviour on exercise.


**Author:** Nour Moustafa & Jill Slay

**Abstract.** One of the major research challenges in this field is the unavailability of a comprehensive network based data set which can reflect modern network traffic scenarios, vast varieties of low footprint intrusions and depth structured information about the network traffic. Evaluating network intrusion detection systems research efforts, KDD98, KDDCUP99 and NSLKDD benchmark data sets were generated a decade ago. However, numerous current studies showed that for the current network threat environment, these data sets do not inclusively reflect network traffic and modern low footprint attacks. Countering the unavailability of network benchmark data set challenges, this paper examines a UNSW-NB15 data set creation. This data set has a hybrid of the real modern normal and the contemporary synthesized attack activities of the network traffic. Existing and novel methods are utilised to generate the features of the UNSW-NB15 data set. This data set is available for research purposes and can be accessed from the link (http://www.cybersecurity.unsw.adfa.edu.au/ADFA%20NB15%20Datasets/).
**1.8b Refereed Papers—INDUSTRY Stream**

**Paper 1: Serving up Data Files to Multiple Classified Networks**  
*Author:* D. Stapleton  
*Abstract.* Today, large and complex geospatial reference files are required on Defence networks of different classifications. This paper proposes a secure mechanism for allowing the same version of a file to be accessed from different classifications, while also providing assurance to users that they are accessing the latest version of that file.

**Paper 2: Preventing Data Spills from Classified Networks**  
*Author:* D. Stapleton  
*Abstract.* When classified files are moved around, from one network to another, often over unclassified networks such as the Internet, they may be protected by simple encryption. This paper proposes a more secure method which ensures that the target network is authorised by the file owner and that access is controlled in an agreed manner.

---

**1.8c Refereed Papers—INDUSTRY Stream**

**Paper 1: Simultaneous X and Ka Band Maritime Satcom Terminal Supporting Both Military and Commercial Ka Band Communications**  
*Author:* John Logan and Chris Leat  
*Abstract.* This paper describes the development and feed testing results of a Tri-band on-the-move (OTM) satellite communications terminal. Using as a baseline an existing gymbal mount and monopulse tracking algorithms, the COTM terminal is being developed for use simultaneously on X-band and Ka-band military satellites and also Ka-band commercial satellites such as Inmarsat GX. The feed has been designed to have monopulse in both X-band and Ka-band (military and commercial) for precise tracking, eliminating the need for mechanical scan tracking methods such as step track or conical scan.

**Paper 2: Break the Stove-pipe Stranglehold on Capability with an Open Systems Approach**  
*Author:* Arthur Ollett and John Coleman  
*Abstract.* Adopting an open systems approach (OSA) during the requirements definition phase of Australian Defence Force (ADF) procurement programs will help break the stove-pipe stranglehold on communication and information system capability. The resulting return on investment will be the delivery of a set of agile capability solutions that are easily enhanced to meet future requirements while at the same time reducing vendor lock-in, risk and support costs. A snapshot of ADF projects are reviewed and we discuss potential strangulation issues regarding ambiguous boundaries and associated risks that could be addressed by an OSA. A brief overview is provided on the OSA initiatives underway by other country’s defence agencies including: UK MOD, US DoD and NATO. We introduce a high level platform concept that could be used as a framework when defining project requirements with an OSA discuss the short and long term benefits that could be achieved. We conclude that an OSA is a future-proofing acquisition strategy that can yield important benefits such as capability gain, more open competition, ability to re-use rather than replace, ultimately reducing waste and lowering costs.
Session Abstracts: Day 2—11 November 2015

2.1 Breakfast Session Product Brief: Senetas and Nextgen Group Partner to Deliver ‘Defence-Grade’ State of the Art Secure Data Centre and Networks Services

Presenter: Julian Fay, Chief Technology Officer, Senetas Corporation

2.2 Plenary Session: Navy, Army, Air Force CIS Interoperability

Moderator: AVM Andrew Dowse, Head ICT Operations, CIOG
Keynote Address: RADM Michael van Balen, Deputy Chief Navy
Keynote Address: MAJGEN Fergus McLachlan, Head Modernisation and Strategic Planning – Army
Keynote Address: AIRCDRE Stephen Osborne, Director-General Strategy and Planning – Air Force

2.3a Plenary Session: Capability Developments

Keynote Address: AVM Mel Hupfeld, Head Capability Systems, CASG
Keynote Address: RADM Peter Quinn, Head Joint Capability Coordination, VCDF Group
Keynote Address: RDML Kathleen Creighton, US PACOM J6
Keynote Address: Mr Victor Vae’au, CIO NZDF

2.3b Lunch Session Product Brief: TBA

Presenter: Mr TBA, TBA

TBA

2.4a Update: MNIS Strategy and Capability Overview

Presenter: Mr Ewart Challis, Director Multinational Relations and Interoperability

This session will provide an overview of the Defence MNIS Strategy and of current and prospective MNIS capabilities.

Defence’s Multi National Information Sharing (MNIS) capabilities enable the electronic exchange of information with mission partners in support of the planning and conduct of coalition operations. MNIS capabilities underwrite Defence’s ability to participate in coalition operations as a peer level mission partner and lead a regional operation with mission partners. Recent operations in Timor Leste and the Middle East have highlighted the need to integrate lessons learned and current information sharing trends into MNIS capability development. The Defence MNIS Strategy was endorsed in 2014 by the Strategic J6, MAJGEN Michael Milford, to provide direction on the future of Defence’s MNIS capabilities.

The Defence MNIS Strategy and Capability Overview session will summarise the key components of the MNIS Strategy and of current and prospective MNIS capabilities. The briefing will include an overview of the current MNIS capabilities available today in support of military operations.

2.4b Update: Changing the face of cyber security

Presenter: Mr Richard Brown, Managing Director of Cogito Group

The number of Cyber incidents has seen a dramatic rise over the last few years and the attacks are becoming more sophisticated.

In most large organisations however, user management and network security are separate siloed teams, resulting in a lack of co-ordination and gaps in the way security is treated across the enterprise.

Organisations that take security seriously now keep boundaries strong, but are prepared for a breach that either occurs through the compromise of the boundary security or the people themselves (the trusted insider).

As internal and external risks grow, we can see data and access to it as the new boundary paradigms. In viewing this way the emphasis changes away from a boundary centric model to a more holistic protection approach. We start to seek to protect the data itself with techniques such as:
• better authentication methods
• better authorisation methods such as better access control through dynamic provisioning and de-provisioning
• seamless encryption.
• the use of identity relationship management to make dynamic access decisions based on dynamic inputs.
• the employment of user managed access where appropriate that extends provisioning to individuals whilst maintaining accountability by all.

This all adds up to addressing security through a layered approach that combines not just boarder protection, but also encryption, access policies, key management, content security and of course, authentication and authorisation. If done well it will also result in not just a more secure environment, but a more flexible and efficient one.

2.4c Product Brief: Cross Domain Guards to Support All Missions

Presenter: Mr Jason Ostermann; Chief Engineer – Transfer Solutions, Raytheon|Websense

Government and commercial entities are constantly on alert to prevent and fight against the ongoing threat of cyber attacks. The dichotomy faced by today’s governments and enterprises is that in order to protect themselves against these threats they must also collaborate and share information across sensitivity levels within their own organizations and also across country and corporate boundaries. In light of this, network security is of paramount significance especially with the keen emphasis currently placed on secure collaboration and information sharing in an environment of increasing threats and vulnerabilities.

In this globally interconnected world it is no longer possible for our people or our technologies to work in isolation. The need to gather and share data across oceans, battlefields, and offices rapidly and securely requires the most robust security solutions. These solutions must also be easy to implement, use and maintain whilst also being cost-effective. Any sophisticated network isolation solution should include multiple layers of defense to provide redundancy and additional monitoring of data flows.

This session will discuss how High Speed Guard™ and Small Format Guard™ from Raytheon|Websense:

• Deliver secure and seamless flow of information between multiple networks, be that machine-to-machine, person-to-machine or machine-to-person.
• Utilize configurable rules to enforce specific flow content and direction controls so that only permissible data is moved from one network to another and only in the prescribed manner.
• Utilize validations to prevent malicious data from entering more secure networks whilst also preventing data leakage from sensitive networks.
• Allow for great flexibility to support many mission types with a single solution.
• Enable cost savings whilst enhancing the security posture

Mr Ostermann holds a TS Clearance with current SSBI and graduated from Texas Tech with a BS in Computer Science. He has 16 years of overall experience in the high tech. industry including network and systems administration, 11 years of experience in guard development; Software Security Engineering and System Administration. Mr Ostermann leads multiple Cross Domain Solution projects and holds CISSP, ISSEP certifications. As the High Speed Guard Chief Engineer, he was responsible for the maturation of a high speed cross domain solution supporting 90% of theoretical line speed throughput for secure data transfers. Jason now brings this experience and talent to the suite of guard technologies at Raytheon|Websense.

2.5a Product Brief: Managing People and Processes Through Roles

Presenter: Mr James Milne, Myriad Technologies

A common challenge faced by modern organisations is to manage employee roles, particularly as people move throughout the organisation. This session will demonstrate some of the benefits of creating a role based hierarchy to manage users, roles and responsibilities, including automated workflows.

As a single point of truth for People, Positions, Places and Roles, Org Connect is the ideal solution to create a role-centric hierarchy. Org Connect enables its users to build adaptive and intelligent business processes which leverage and unlock this "people information". The product empowers its users with the information and automation they need to enhance their productivity in the workplace.

2.5b Product Brief: The Case for Secure Mobility in Defence

Presenter: Mr Jon Green, CTO, Aruba Networks Government Solutions
In a world where the timely delivery of information is pivotal to the success or failure of an operation, where we need to deliver said information to a mobile task force that is constantly on the move whilst at the same time being constrained by expenditure, we need to consider commercial-off-the-shelf secure mobility solutions that deliver on outcomes.

What do we mean by “Mobility”? Some people immediately think LTE/cellular when they hear the term, whilst others look to Wi-Fi, VDI or published apps as a way of getting applications and information onto “any device, anywhere, anytime”.

What benefits does Mobility bring? Embracing this shift can certainly be advantageous—especially in today’s world where bandwidth and optimisation has reached a stage where we can successfully deliver real-time, bandwidth intensive content easily.

However, what are the risks and how do we deal with security? In this modern age where people are connected across the globe we are becoming increasingly security conscious and traditional methods may no longer be sufficient. We now look to secure not only the communication path and information but also obscure the location of the individual and the device.

We are not alone in our concerns. Every sovereign nation and most organisations on this planet are trying to find the right balance between security and mobility, by weighing up the respective benefits and risks.

In this session we will aim to answer some of these key questions by exploring what other military & government organisations are doing in the Mobility space. The paths considered by these entities help provide insight into how we can embrace the inevitable mobility trend.

**2.5c Product Brief: TBA**

Presenter: Mr TBA, TBA

TBA.

**2.6a Update: Defence Spectrum Strategy**

Presenter: Mr Alex Wright, Spectrum Engineer, CIOG - Defence Spectrum Office

This presentation will provide an overview of the Defence Spectrum Strategy, including:

- Background and Need for a Spectrum Strategy, covering the Defence enterprise.
- Drivers of supply and demand for Defence Spectrum Access.
- Goals of the Strategy:
  - Influence – To influence national & international Spectrum Management policy and ensure Defence requirements are represented
  - Govern – To institutionalise a cohesive, Enterprise-wide Spectrum Lifecycle Management approach.
  - Manage – To manage the delivery of Spectrum Access to support Defence operations and deliver commitments as directed by government
  - Innovate – To pursue innovative approaches for the efficient, resilient and adaptable use of Spectrum
  - Objectives of the Spectrum Strategy.
- Implementation Plans.
- Frontier topics, such as Defence sharing of spectrum and the overlap of Spectrum Management, Electronic Warfare and Cyber.

**2.6b Update: Government Spectrum Review – Implications for Defence**

Presenter: Mr Alex Wright, Spectrum Engineer, CIOG - Defence Spectrum Office

The Australian Spectrum Regulatory framework comprises core legislation such as the Radiocommunications Act 1992 (as amended) and numerous supporting legislative instruments, including the Australian Radiofrequency Spectrum Plan (ARSP).

A review into this framework was undertaken during 2014-15 by the Department of Communications, supported by the Australian Communications and Media Authority (ACMA).

The review report was released in May 2015. This presentation will discuss:

- Current arrangements for spectrum used by Defence, including fee payments.
• The recommendations of the review, including:
  • Replacing the current legislative framework.
  • Improving the integrity and consistency of the framework and better integrating public sector agencies (such as Defence).
  • A further review to consider spectrum pricing arrangements.
  • Potential implications for Defence, such as:
    • ACMA delegation to Defence as a frequency “Band Manager”, for specific bands.
    • Defence sharing of particular frequency bands with other users/users.
    • Increased emphasis on status accounting and reporting for Defence use of any spectrum.
    • ACMA devolving responsibility for resolving interference issues to spectrum users.
    • Increasing complexity of spectrum management and increased spectrum licencing costs.
  • Implementation Plans for the Review.

2.6c Update: Update on CIS Trials at Talisman Sabre

Presenter: Mr TBA, Land Network Integration Centre

2.7a Product Brief: Next Generation Mobile Intelligence: Dynamic Collaboration Solutions

Presenter: Mr Graeme Stanley, Public Safety Solutions, Motorola Solutions

Rapid advances in technology are creating revolutionary capabilities for defence and public safety agencies. For these agencies, the ability to dynamically collaborate in real-time, capturing and securely sharing intelligence across agencies can mean the difference between mission success and failure.

**DragonForce - team collaboration application: bring different agencies together as a team for effective, coordinated response**

Create enhanced situational awareness through real time personnel tracking, shared maps, floor plans and images for improved tactical and emergency response in the command centre and the field. This collaborative mapping and whiteboard application means all responders have a single operating picture with real time intelligence to accomplish their mission.

**WAVE 5000: every device, every network, every team, connected like never before**

WAVE 5000 is a communications interoperability and broadband push-to-talk (PTT) solution that delivers real-time voice and data securely over any network using any device.

Created by Motorola’s wholly owned subsidiary Twister Pair, ongoing product development and enhancements allow WAVE 5000 to enable highly scalable, feature rich, push-to-talk (PTT), so critical, time-sensitive information flows quickly and securely between responders.

From two-way radios to smartphones, laptops to landlines, tablets to rugged handhelds, WAVE 5000 lets users use the devices they already have and the networks they already subscribe to, to connect and talk.

**Intelligent Data Portal – put actionable intelligence in the hands of responders**

Intelligence Data Portal is a cloud-based mobile application that gathers location based information from disparate databases and organises it on a real-time map for improved situational awareness and strategic planning.

Hear how these next generation solutions are transforming the way defence and public safety agencies respond.

2.7b Product Brief: TBA

Presenter: Mr TBA, TBA

TBA

2.7c Product Brief: TBA

Presenter: Mr TBA, TBA

TBA
2.8a Refereed Papers—Industry Stream

Paper 1: Symmetrical Data Link for Burst Mode Transmission
Authors: Ajit Reddy
Abstract. In this paper we discuss the architecture and the implementation of 5 Mbps over the air data rate, burst mode data link which has the capabilities of the upstream and downstream transmission in a single module with symmetrical data rates in time division duplex (TDD) manner. The data link operates in the S band. In this paper, we discuss the various RF challenges that exist on a RF system-level and show how such challenges can translate into implementable circuit designs. The reason for a TDD based RF front end is that TDD is known to offer cost advantages as compared to FDD based system. The additional advantage is that it uses less space compared to FDD and where size is an issue. The fundamental subsystem blocks such as synthesizers, filters and power amplifiers are where most of the RF front end transceiver costs reside. We also discuss some of the important modem specifications for RF and baseband and the implications for the design of RF circuits, which include SNR, channel bandwidths, RF bands, noise figures, output power levels, and gain setting.

Paper 2: Validation of MUF and FOT Parameters for Plain, Mountainous and Sea Region
Authors: Mansoor Ahmad
Abstract. In this paper, the validation of different International High Frequency (HF) prediction models for HF communication in plain, mountainous and sea regions of Pakistan are studied. An analytical study for the behaviour of Ionospheric parameters, Maximum Usable Frequency (MUF) and Frequency of Optimum Traffic (FOT) has been performed between transmitter station Lahore City and many different receiver stations which are distributed randomly over Pakistani territory. The Ionospheric parameters are calculated using Ionospheric Communications Enhanced Profile Analysis & Circuit (ICEPAC) and REC 533 communication models for all seasons (Summer, Winter, Autumn and Spring) of the year 2013 of the solar cycle 24. Before this study no single model was followed properly for HF communication frequency prediction to meet the requirements of this complex geographical location containing plain, mountainous and sea regions. A comparison of practical and theoretical results shows that ICEPAC model results shows best fitting to plain, mountainous and sea regions of Pakistan as compared to REC 533.

2.8b Refereed Papers—Industry Stream

Paper 1: Miniaturized Wideband Branch-Line Hybrid Coupler with Four Pine Shape Capacitive Effect
Authors: Pejman Mohammadi
Abstract. In this paper a novel 3dB miniaturized broadband branch-line coupler is designed and experimentally verified. The new distributed capacitors which are placed within the empty space of the hybrid, minimize the size of the coupler. A prototype at 2.5GHz was designed and built. Measurement result confirmed that there is 2700 phase difference between output ports. The size of fabricated modified structure shows 55% reduction with respect to conventional 3dB branch line coupler and also the measured bandwidth is 0.5 GHz.

Paper 2: Design and Simulation of Digital Down Converter for SOQPSK Wideband Heterodyne Receiver
Authors: Ajit Reddy
Abstract. In this paper we present the design and simulation for digitally down converting the SOQPSK signal from IF to baseband in a wideband heterodyne receiver. The receiver operates in the S band and uses a bandwidth of 6 MHz. The intermediate frequency (IF) stage is at 140 MHz. The architecture presented uses an IF sub-sampled digital down conversion to demodulate the SOQPSK signal from IF to baseband

2.8c Tutorial: Wireless Backhaul—A Primer on Microwave and Satellite Communications
Presenter: Mr Rowan Gilmore, CEO, EM Solutions Pty Ltd

Point to point microwave radio links and satellite communications might appear to be a world apart, but both can be used for backhaul of high speed data, and both share common features.

This tutorial is an introduction to the radio air interface (the physical layer) and to how wireless backhaul works, and by comparing terrestrial and satellite communications links, shows the trade-offs in typical communications systems.

Starting with Shannon’s equation, the fundamental trade-offs between bandwidth, power, noise and system capacity are first explored. Next, the components of both terrestrial and satellite link budgets are examined, and the trade-offs between distance, gain, antenna size, and modulation at various frequency bands are picked apart. The effects of mobility, weather, fading, and multi-path interference are discussed, and different types of modulation schemes to preserve bandwidth at the expense of sensitivity are simulated. Comparisons between terrestrial and satellite communications are used to illustrate the key principles.
Finally, typical commercial radio system architectures for both terrestrial and satellite terminals are shown and simulated to illustrate how system imperfections, such as linearity and noise, can degrade the bit error rate and link performance, and to show why poorly designed systems are more susceptible to jamming signals and interference than others.

The tutorial is a refresher for communications engineers, field personnel, and procurement and project managers.

Presenter: Mr James de Vroome, Business Development Manager – Enterprise & Government, Pivotel

Pivotel Group is an Australian owned and operated satellite communications company offering a secure, reliable Australian satellite network across a range of satellite service providers. With network interconnect points across Australia users can rely on their connection to the Pivotel Network Gateway to transmit sensitive information quickly and securely.

Pivotel’s new Push-to-talk (PTT) service using the Iridium Satellite Network takes push-to-talk communications to the next level. Remote Defence personnel often require a fast, reliable and secure communication channel for one-to-many voice communications when making a one-to-one satellite call is not time-effective. The PTT service allows a group of users to communicate in the same way they would use push-to-talk radio services, but using a secure, reliable satellite connection. Using specially configured Iridium Extreme satellite handsets, a group of users within a specified geographic footprint can simply push a button to broadcast a message to the other users within their talk group.

The Iridium Satellite Network offers truly global coverage and its Low Earth Orbit (LEO) satellite constellation provides a fast PTT service with very low latency. Iridium’s PTT is secure; it uses AES256 encryption to transport all PTT voice content; AES256 is one of the top encryptions in use and is currently used by the leading Governments when transmitting top secret data. The PTT service is affordable and flexible, with the ability to configure handsets within a group easily and quickly.

3.2 Plenary Session: Defence Cyber

Keynote Address: TBA, Australian Signals Directorate, I&S Group
Keynote Address: Mr Greg Gale, A/Assistant Secretary ICT Security, CIOG
Keynote Address: GPCAPT Paul Wade, Director Defence Cyber Coordination Office, VCDF Group

3.3a Plenary Session: SecureCanberra Plenary

Welcome Address: W. Hord Tipton, Executive Director, (ISC)², Former CIO, U.S. Department of the Interior, U.S.A

Keynote Address: Resilient Systems and Cyber Missions: Dr Mike Davies, Research Leader, Cyber Assurance and Operations, Cyber and EW Division, Defence Science and Technology Organisation

Keynote Address: Forensics in the Cloud: Prof. Jill Slay, Director, Australian Centre for Cyber Security, School of Engineering and Information Technology, University of New South Wales

3.3b Lunch Session Product Brief: Tactical Advantage for Data Management at Scale and Gaining Value

Presenter: Mr Callan Fox, Emerging Technologies Division, EMC Global Holdings

This session will explore a storage solution which makes managing large datasets at scale easy, while providing out-of-the-box integration with analytics platforms to gain intelligence from the data in place.

The sheer amount and ever-increasing sophistication of information can overwhelm analysis systems and processes. Data from sources as varied as unmanned aerial vehicles, surveillance video, network devices and online chat result in a constant flood of information so vast that only a fraction of it can be analysed quickly. The Intelligence, Surveillance and Reconnaissance (ISR) community are struggling to develop capabilities to analyse intelligence at an unprecedented speed and capacity. The growth in the number of UAVs collecting intelligence is exponential. Airborne sensors now track dozens of targets simultaneously. UAVs feed full-motion video directly to front-line troops. Automated systems suction emails, chats and Twitter feeds continuously from the ether, forming constellations of sensors and sensor networks. The problem of collection has largely been addressed, but has created massive challenges related to storing and analysing data, and to disseminate useful intelligence.
3.4a SecureCanberra Track

Optimising Cyber Security Learning Through Hands-on and Role-play Approach
Presenter:  Mr Jimmy Ng Wee Kok, NEC

Developing an Architectural Framework Towards Achieving Cyber Resiliency
Presenter:  Deepak Singh, Head of Professional Services, Secure Logic

3.4b SecureCanberra Track

The Changing Landscape: The Internet of Things
Presenter:  Professor Sanjay Jha, University of New South Wales

Using Big Data to Secure Your Enterprise
Presenter:  Mr Matt Carling, Cisco Australia

3.4c SecureCanberra Track

The Changing Landscape: The Internet of Things
Presenter:  Professor Sanjay Jha, University of New South Wales

Using Big Data to Secure Your Enterprise
Presenter:  Mr Matt Carling, Cisco Australia

3.5a Product Brief: Harris Next Generation C2ISR Capabilities
Presenter:  Mr Adrian Craven, Major Accounts Manager - Asia Pacific, Harris Software Systems Pty Ltd

During this presentation, Harris will provide an overview of its next generation of product lines across the Communications and Surveillance capability lines as well as an update on US DOD waveform developments.

3.5b Product Brief: Icom Australia: For Everything in Radio
Presenter:  Mr Grant Fernando, Quality Assurance Manager, Icom Australia

Icom Australia is a world-class manufacturer of wireless communication products throughout Australia and the Pacific Islands. Icom Australia’s unsurpassed reliable communication equipment provides solutions to a number of unique business problems, leveraging dedication to quality, innovation, performance and simplicity of operation. Established in 1982, Icom Australia has developed an extensive product range, supplying radio communications in the avionics, amateur, marine, land mobile, UHF CB and wide receiver industries. The comprehensive range means Icom Australia can tailor communication equipment to suit individual and unique business needs.

Icom Australia have pioneered innovations in the Radio over IP (ROIP) market by developing a full-duplex, secure radio communications system that works over wireless LAN and IP networks. Defence personnel require reliable and secure communications for one-to-many voice communications and Icom’s IP Advanced Radio System is secure; it uses WPA-PSK and WPA2-PSK to encrypt private conversations. The real power of Icom’s IP Advanced Radio System is maximised when users interface Icom’s VE-PG3 (Radio over IP Gateway) which provides integration into many different technologies such as traditional R.F radio (analogue and digital), airband, H.F, Sip/IP phones, PSTN phone and mobile integration and marine radios. With the addition of a VPN router, users are able to interface a link to provide area coverage anywhere in the country and the world.

This brief will outline the importance of ROIP to military and intelligence users and how this technology is at the forefront of assisting the Defence to move to a more efficient radio network infrastructure.

3.5c Update: New Antennas for New Battlefields; EW Antennas—A Platform Capability
Presenter:  David Benchoam, General Manager, Benelec Pty Ltd

New Antennas for New Battlefields: EW Antennas – A Platform Capability is the second Technology White Paper prepared by Benelec Pty Ltd for MilCIS. The first White Paper discussed the design of new C2 and EW antennas to meet the demands of the modern battlefield The second White Paper discusses the changing requirement for high-performance EW antennas that are integrated on platforms, and which enhance the capability of personnel, vehicles, ships, temporary land installations and permanent land installations. The EW antennas must be capable of meeting the
dual roles of force protection against IED and other weapon systems, and to provide radio frequency (RF) situational awareness through interception.

The White Paper identifies changing needs for EW antennas: defeating a clever enemy with the latest telephone and radio systems; integrating EW, C2 and weapons systems on platforms; minimising disruption on C2 and intercept communications from jammers; protecting ECM systems from attack; minimising jammer effects on civilian communications. This requires new approaches to concepts, design, evaluation and manufacture. These include: covering wider frequency bands to include known mobile telephone and radio systems; high performance operation to deliver effective intercept and jamming signal strengths; optimise and not impede the physical fighting capabilities of the specific platform; avoid disrupting other RF and electronic systems on the platform; minimise demands on external ‘real estate’ and internal cable space on the platform; minimise the potential effects of spurious RF radiation on personnel; and be robust enough to continue operating in extreme combat situations.

3.6a Tutorial: Document and Records Management in SharePoint

Presenter: Mr James Milne, Myriad Technologies

From the point of creation through to eventual disposal, an organisation’s business information needs to be managed, protected, secure and easily accessible. With unprecedented growth in electronic information it becomes exceedingly difficult for an organisation effectively manage that information. The complexities occur when determining what information to trust, keep, secure, and of course, discard. In this session we will demonstrate the technology available today that can make managing, finding and securing information efficient and seamless.

3.6b Tutorial: Replication in the field

Presenter: Mr James Milne, Myriad Technologies

Some of the key challenges facing organisations today is the geographically dispersed networks both in Australia and abroad, as well as limited network connectivity and availability. Sharing information in these hostile environments has previously been limited and the need to exchange information about operations in the field is critical. This session will demonstrate how Microsoft SharePoint 2013 combined with replication technology can be utilised to allow collaboration on documents in multiple locations regardless of the network status.

3.6c Tutorial: Building electronic forms and workflows to streamline your business processes

Presenter: Mr James Milne, Myriad Technologies

This session will demonstrate how SharePoint and Nintex Workflows can be used to automate business processes both within the organisation and in the field. This session will allow participants build an electronic form and create the workflow behind the form to ensure the business process completes in a timely manner. Using SharePoint and Nintex Workflows can dramatically change the way organisations streamline business processes.

3.7a Update: Centralised Processing – Transformation

Presenter: Ms Julie Bance, Lockheed Martin Australia and Ms Janice Law, CIOG

TBA

3.7b Update: Military CIS Workforce Demographics

Presenter: Robert Kremer, Director, Kinetic Defence Services Pty Ltd

Background: Australia is embarking upon a large number of C4I related projects, and a skilled workforce is needed to design, integrate and sustain these new capabilities. In the past, Defence project delivery and platform availability has been put at risk through the unavailability of suitable workers. Kinetic Recruitment publishes the only Defence skills specific salary and demographic information in Australia.

Results: The 2015 survey showed that the salary levels for certain security cleared skill sets in the CIS sector have increased significantly over the last 24 months. Business Analyst salaries have increased by as much as 57%, depending on the level of experience and clearance, and salaries for Security Consultants have increased by up to 30% over the period. This is well above the average increase in Australian salaries for the period of under 3%.

The aging workforce will also effect the supply of workers, with 22% of workers aged over 55. This statistic also supports the observation that many younger workers did not join the defence industry over the last 10 years due to competition from other sectors or constrained capacity to grow defence industry workforces. This is particularly true of some CIS skill sets.
Conclusion: In an environment of potentially high demand for CIS workers, significant project risk will develop should workers with suitable skills not be available. Government and industry will need to learn from experience and prepare carefully to manage the supply and demand of workers.

3.7c Update: TBA

Presenters: TBA, TBA

TBA

3.8a Tutorial: Establishing a Flexible, Open Cyberinfrastructure Framework for Virtual Organizations

Presenter: Dr Morcosu Massoud, Cairo University

With access to state-of-the-art cyberinfrastructure services, many researchers and indeed entire fields of science and engineering now share access to world-class resources spanning experimental facilities and field equipment, distributed instrumentation, sensor networks and arrays, mobile research platforms, HPC systems, data collections, sophisticated analysis and visualization facilities, and advanced simulation tools. The convergence of information, grid, and networking technologies with contemporary communications now enables science and engineering communities to pursue their research and learning goals in real-time and without regard to geography. In fact, the creation of end-to-end cyberinfrastructure systems – comprehensive networked resources – by groups of individuals with common interests is permitting the establishment of Virtual Organizations (VOs) that are revolutionizing the conduct of science and engineering research and education. Such virtual organizations supporting distributed communities go by numerous names: collaborator, grid community, science gateway, science portal, and others. During the past decade, NSF funding has catalyzed the creation of VOs across a broad spectrum of science and engineering fields, creating powerful and broadly accessible pathways to accelerate the transformation of research outcomes into knowledge, products, services, and new opportunities. With access to enabling tools and services, self-organizing communities can create end-to-end systems to: facilitate scientific workflows; collaborate on experimental designs; share information and knowledge; remotely operate instrumentation; run numerical simulations using computing resources ranging from desktop computers to HPC systems; archive, e-publish, access, mine, analyze, and visualize data; develop new computational models; and deliver unique learning and workforce development activities. Through VOs, researchers are exploring science and engineering phenomena in unprecedented ways. To catalyze the development, implementation and evolution of a functionally complete national cyberinfrastructure that integrates both physical and cyberinfrastructure assets and services to support VOs. To promote and support the establishment of world-class VOs that are secure, efficient, reliable, accessible, usable, pervasive, persistent and interoperable, and that are able to exploit the full range of research and education tools available at any given time. To support the development of common cyberinfrastructure resources, services, and tools enabling the effective, efficient creation and operation of end-to-end cyberinfrastructure systems for and across all science and engineering fields, nationally and internationally.