MISSION TO SINGAPORE, THE NETHERLANDS AND UNITED STATES OF AMERICA

THE HONOURABLE TROY GRANT MP

Minister for Police and Minister for Emergency Services

30 September – 9 October 2017

MISSION REPORT

PURPOSE

The Department of Justice is currently embarking on an ambitious program of reform to enhance biometric capabilities, cyber-security and cyber-safety.

The widespread use of the internet as an everyday commodity and sophistication of its use by organised crime networks has reinforced the need for global security. It has given rise to new threats that are now common to both the public and private sectors. Law enforcement agencies within Singapore, the European Union and the USA have implemented a series of best practice tools and frameworks in response to the growing threat of terrorism and evolution of cybercrime and cyber enabled transnational crime. The purpose of this trip was to gain a stronger understanding of world renowned approaches in those countries to enhance cyber-safety and security, biometrics and counter terrorism capabilities in NSW.

OFFICIAL DELEGATION

The Honourable Troy Grant MP
Minister for Police and Minister for Emergency Services

Accompanied by:

Arthur Katsogiannis
Detective Superintendent, Commander, Fraud and Cyber Crime Squad, NSW Police Force

Adrian McKenna
Executive Director, Office for Police, NSW Department of Justice

Rachael Hayes
Deputy Chief of Staff, Office of the Minister for Police and Minister for Emergency Services

Chris Craner
Chief Superintendent, Chief of Staff Office of the Commissioner, NSW Police Force

MISSION DESCRIPTION

The Department of Justice in conjunction with the Australian Federal Police (AFP) stationed in the Netherlands organised briefings, meetings and demonstrations with units and teams within EUROPOL relevant to cyber-security and crime, counter terrorism and biometrics. EUROPOL is an international policing organisation that focuses on law enforcement, intelligence collection, analysis and information sharing.

The Department of Justice also made arrangements for meetings and demonstrations with the Cybercrime Directorate of INTERPOL and the New York Police Department.

These briefings delivered valuable insight on the resourcing requirements and functionality for cyber-security/crime and biometric operational units which have greatly assisted in the development of operational allocations for the NSW Police Force currently underway.

Activities

A selection of notable meetings are listed below:

Meeting	Purpose of Meeting / Learnings
Manuel Navarrete Paniagua, Head of Europol Counter Terrorism Centre	Inter-government and inter-agency coordination on detection of cybercrime, online terrorist propaganda and extremism, counter terrorism intelligence management.
Rob Wainwright, Director of Europol	Insights into partnership and cooperation with NSW Police Force and AFP.
Presentation by the Internet Referral Unit, Europol	Exposure to current operations and effective organisational structures, detection and provision of strategic and operational analysis and information sharing.
High Tech Crime Centre, the Netherlands Police	Insights into detection, infiltration and prosecution against illegal marketplaces on the dark web.
Meeting with John Rieman, NPN Specialist involved in Biometrics and administrator of the HAVANK database	Insights into the use of biometrics for the purposes of law enforcement.
Steven Wilson, Head of Cybercrime, Europol	Insight into the current challenges in detecting cybercrime, detection and identification strategies, resourcing and effective organisational structures.
NYPD Facial Recognition Unit	Applications and challenges with facial biometric technology, resourcing and effective organisational structures.
National Cyber-Forensics & Training Alliance Meeting.	Effective organisational structures for cyber-crime and forensic analysis unit. Insights into partnership and cooperation with NSW Police Force.

KEY OUTCOMES

The meetings provided opportunities to deepen our understanding of the challenges and effective strategies to improve the capacity of law enforcement agencies to investigate and prosecute cybercrime and 'technology-assisted crime' and counter-terrorism. They also provided information regarding international responses to major events and incidents, including effective inter-government and inter-agency coordination and information sharing, and a detailed insight to effective organisational structures.

Meetings were held with the Executive Director of Europol, the Head of Cybercrime and Director of the Counter Terrorism Centre at Europol as well as the representatives from the NYPD Police Headquarters and specialist support.

The delegation ascertained a number of insights into the operations and effective use of tools and models during the meetings and briefings with the various law enforcement agencies. A consistent trend observed across the agencies was the vision and level of importance placed on modernised partnerships, the need to share the right information, and collaboration under a global platform that transcends national and regional efforts. Access to the right data from private and public partners, within agreed parameters that are mutually respected was also observed to be critical solving cybercrimes, improving cyber security and countering terrorism.

A modernised approach to current operations, as well as the need to further strengthen and equip the NSW Police Force (NSWPF) with sophisticated operational tools and utilities is necessary to stay ahead of terrorists and criminals that seek to circumvent lawful processes in the form of identity fraud, cybercrime, cyber-enabled crime and terrorism.

With these learnings in mind, the below outlines actions to be further progressed via the Department of Justice:

1. *Facial Biometric Recognition Capability*

   All Australian jurisdictions signed the Intergovernmental Agreement on Identity Matching Services (IMS IGA) at a special COAG meeting in October which will result in NSW integrating with the National Facial Biometric Matching Capability (the Capability). The Capability will enable facial matching of biometric data held by participating jurisdictions' agencies (e.g. passports, immigration photos and drivers licences).

   Eventually the Biometric Capability will connect each identity database in Australia, for example the NSW driver licence database. Recent recommendations from the Lindt Siege Report highlighted the need for the NSWPF to be able to identify victims and perpetrators more quickly. This technology will help the NSWPF achieve this by using facial recognition to confirm people's identity.

   The Department of Justice will lead the implementation of the matching services and oversee integration into NSW current business processes, establish an ongoing auditing regime, provide performance analysis, calibrate biometric templates and provide advice on biometric technology and its development.

2. *Cybercrime and Cybersecurity*

The current review of the NSW Crime Commission (NSWCC) will consider changes to the existing organisation's structure to improve its capability and capacity to detect, disrupt, investigate and prosecute cybercrime and manage digital evidence.

We must also consider how best to support cybercrime functions within NSW law enforcement with appropriately skilled officers that will be well versed in the workings of cyber forensics, hacktivism, malware exploits, ransom ware and online fraud. This should also include language and cultural identity experts with the ability to translate and interpret global cyber intelligence, including those that may overlap with terrorist links or radicalisation.

The Department of Justice and NSWPF will be key contributors to the development of the NSW Cyber Security Strategy to ensure a co-ordinated and effective approach to dealing with the challenge of cyber-security, given the far-reaching and costly impacts of service and information loss, corruption or breaches.

3. *Community and Private Sector Collaboration*

The Department of Justice and NSWPF are currently investigating community policing initiatives and strategic partnerships to improve and enable the sharing of information between private sector, trusted businesses and personnel in an effort to support initiatives towards counter terrorism, crime prevention (cyber and cyber-enabled) and community safety. This recognises private sector personnel as a force multiplier in the fight against terrorism, cyber-attacks and security and the importance of sharing critical information in a timely and modernised manner.

Estimated Costs and Details of the Minister's Mission

Minister	Minister Troy Grant
Portfolio	Police and Emergency Services
Destination(s) visited (a) Countries (b) Cities	 (a) Singapore, Netherlands, USA (b) Singapore, The Hague, New York, Pittsburgh
Dates of travel (a) Departure date (b) Return Date	 30 September 2017 9 October 2017
Number of official travel days	10
Number of accompanying (a) Minister's Staff (b) Government Officials	 1 3
Costs	
Airfares (a) Minister and Minister's staff (b) Government Officials	 (a) $13,275.40 (b) $20,181.20
Accommodation (includes any meals/incidentals charges to room) (a) Minister and Minister's staff (b) Government Officials	 (a) $5,845.54 (b) $9,317.68
Official hospitality a) Minister and Minister's staff b) Government officials	 (a) Nil (b) Nil
Other expenses (a) Official gift presentation (b) Ground transport (c) Meals and Refreshments (d) Other miscellaneous costs	 (a) Nil (b) $1136.54 (c) $1280.82 (d) $Nil
TOTAL estimated travel cost (a) Minister and Minister's staff (b) Government officials	 (a) $19,509.76 (b) $31,527.42
Currency conversion rate	1 AUD = 1.063 SGD 1 AUD = 0.67 Euro 1 AUD = 0.78 USD

Note: the above costs are estimates. Currency conversion costs estimates are based on an average exchange rate. Actual costs may vary slightly.

This report does not include costs for data roaming, official passports, visas, vaccinations, insurance, translation or printing of business cards.